

普通高等教育“十一五”国家级规划教材　计算机系列教材

Windows 网络管理简明教程

杨杰　崔建涛　王华东　等编著

清华大学出版社

计算机系列教材

Windows网络管理简明教程

杨　杰　崔建涛　王华东　等编著

清华大学出版社

北　京

内 容 简 介

本书是 Windows 网络管理的简明教程，主要以 Windows Server 2003 为例，介绍了 Windows 网络管理概述、NTFS 文件系统、磁盘管理，深入讲解了活动目录服务、账户管理、组织单位和组策略，重点讲解了如何实现 DNS 服务器、DHCP 服务器、Web 服务器、远程访问与虚拟专用网、Windows 路由与 NAT、终端服务与远程桌面等典型网络服务。

本书内容简明扼要，突出系统性、实用性和可操作性，重点讲解网络管理员必备的基础知识和操作技能，读者很容易根据书中的步骤完成 Windows 常见的网络管理任务。

本书的作者有丰富的教学经验、网络配置与管理的实际工程经验，本书既可作为高等学校计算机科学与技术、软件工程、网络工程等相关专业的操作系统实践教材，也可作为网络设计与管理技术人员的参考书。

图书在版编目（CIP）数据

Windows 网络管理简明教程/杨杰等编著. —北京：清华大学出版社，2015
计算机系列教材
ISBN 978-7-302-40893-2

Ⅰ. ①W…　Ⅱ. ①杨…　Ⅲ. ①Windows 操作系统—网络服务器—高等学校—教材　Ⅳ. ①TP316.86

中国版本图书馆 CIP 数据核字(2015)第 165872 号

责任编辑：白立军
封面设计：常雪影
责任校对：白　蕾
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.75　　**字　　数**：387 千字
版　　次：2015 年 9 月第 1 版　　**印　　次**：2015 年 9 月第1 次印刷
印　　数：1～2000
定　　价：29.50 元

产品编号：065568-01

前 言

Windows 操作系统作为当今主流的窗口操作系统，由于其操作直观、简便，深受广大用户的青睐。Microsoft 公司推出的 Windows Server 2003 是在 Windows Server 2000 的基础上发展而来的，系统更加稳定，功能更加强大，Windows 服务器也成为当今中、小企业首选的服务器。

本书是 Windows 网络管理的简明教程，主要以 Windows Server 2003 为例，介绍 Windows 网络管理概述、NTFS 文件系统、磁盘管理，深入讲解了活动目录服务、账户管理、组织单位和组策略，重点讲解如何实现 DNS 服务器、DHCP 服务器、Web 服务器、远程访问与虚拟专用网、Windows 路由与 NAT、终端服务与远程桌面等典型网络服务。

本书面向网络设计与管理的入门者，旨在使读者学习完本书后，学会 Windows 网络操作系统的使用，掌握常用网络服务的概念，利用 Windows Server 2003 构建企业内部网络，以便为学习其他网络操作系统打下基础。本书尽可能通过实例来讲解 Windows 常见网络管理和典型网络服务的配置。

在教材内容深浅程度上，坚持理论够用、侧重实践、由浅入深的原则。作为教材，学习本书所需的课时约为 30 理论学时、20 实验学时。

本书由杨杰、崔建涛任主编，王华东任副主编。参与本书编写的有郑州轻工业学院的杨杰、崔建涛、王华东、张玲、孙海燕、杨华、崔霄。在本书的编写过程中，得到了郑州轻工业学院和清华大学出版社的大力支持，在此表示感谢。

由于编者水平有限，书中难免存在疏漏之处，敬请广大读者批评指正。

编　者

2015 年 6 月于郑州

目 录《Windows 网络管理简明教程》

第 1 章　Windows 网络管理概述

学习目标

学习完本章后，能够了解 Windows Server 2003 增强功能、版本、网络管理任务以及大型网络中常见的服务器角色，熟悉 TCP/IP，掌握 TCP/IP 诊断、连接工具的使用方法，理解工作组结构、域结构网络的特征，掌握 Windows Server 2003 网络及防火墙设置。

1.1　Windows Server 2003 概述

1.1.1　Windows Server 2003 增强功能

Windows Server 2003 为用户提供了多任务、内存支持、对称多处理、即插即用、群集、文件系统功能、服务质量、终端服务和远程安装服务等增强功能。

(1) 多任务。多任务使用户能在一个系统上同时运行多个应用程序。用户可以同时运行的应用程序数量以及运行这些程序时的系统性能取决于系统内存的大小。

(2) 内存支持。每个在 Windows Server 2003 上运行的应用程序都需要一定的内存来运行。为了支持同时运行多个应用程序和需要大量内存的应用程序，Windows Server 2003(32 位版本)提供了对多达 64GB 内存的支持。

(3) 对称多处理。对称多处理(SMP)是一种技术，它允许操作系统同时使用多个处理器，通过缩短事务处理时间来改进性能。根据版本不同，Windows Server 2003 可以对多达 32 个处理器的 SMP 提供支持。

(4) 即插即用。即插即用设备在插入计算机后可以立即使用，而不需要执行复杂的安装过程，Windows Server 2003 会自动识别新增的硬件并完成其配置。

(5) 群集。Windows Server 2003 可以组合一组独立的计算机来运行一组应用程序。这个组合对于客户端和应用程序就像是一个单独的系统，这个功能被称为群集。这种方式可以防止单点失败。例如，如果一台计算机发生问题，群集里的另一台计算机将代替它提供相同的服务。

(6) 文件系统功能。Windows Server 2003 支持 3 种文件系统：FAT、FAT32 和 NTFS 文件系统。一般情况下，在配置为双重启动的计算机上才使用 FAT 或 FAT32 文件系统，NTFS 是 Microsoft 公司建议使用的文件系统，NTFS 提供文件系统恢复、大容量分区、安全性、磁盘配额、压缩等功能。

(7) 服务质量(QoS)。在 Windows Server 2003 中，服务质量(QoS)是一系列服务要求，网络必须满足这些要求才能保证一定的数据传输服务水平。QoS 可以控制分配给应用程序的网络带宽，保证端到端的快速传输信息。

(8) 终端服务。终端服务可以让用户如同访问本地计算机一样访问远程计算机。用

户可以通过使用终端服务来运行服务器上的应用程序，也可以从网络上的任何地方对服务器进行管理。使用终端服务可以减少网络的总体运行成本。

(9) 远程安装服务。远程安装服务使管理员能在整个企业内部很方便地远程部署操作系统。

1.1.2 Windows Server 2003 版本

Windows Server 2003 分为以下 4 个版本。

1. Windows Server 2003 Web 版

该产品专门针对 Web 服务优化，特别适用于构建网站，为采用 ASP.NET 技术的网站与应用程序提供了一个快速开发与构建的平台。该产品支持双路处理器、2GB 内存，同时支持 ASP.NET、DFS 分布式文件系统、EFS 文件加密系统、IIS 6.0、智能镜像、ICF 因特网防火墙、IPv6、Microsoft.Net Framework、NLB 网络负载均衡、PKI、Print Services for UNIX、RDP、远程 OS 安装（非 RIS 服务）、RSoP 策略的结果集、影子复制恢复（Shadow Copy Restore）、VPN 和 WMI 命令行模式等功能。此版本仅能够在活动目录域中作为成员服务器，而不能够作为域控制器。

2. Windows Server 2003 标准版

该产品是针对中小型企业的核心产品。支持双路处理器、4GB 内存。除了具备 Windows Server 2003 Web 版的所有功能外，还支持证书服务、UDDI 服务、传真服务、IAS 因特网验证服务、可移动存储、RIS、智能卡、终端服务、WMS 和 Services for Macintosh 等。

3. Windows Server 2003 企业版

该产品被定义为新一代高端产品。最多能够支持 8 路处理器、32GB 内存和 2～8 个节点的集群。它是 Windows Server 2003 Standard 版的扩展版本，增加了 Meta Directory Services Support、终端服务会话目录、集群、热添加（Hot-Add）内存和 NUMA 非统一内存访问存取技术。这个版本还增加了一个支持 64 位计算的版本。

4. Windows Server 2003 Datacenter 版

该产品代表 Microsoft 公司最高性能的产品，定位于最高端的应用，有着极其可靠的稳定性和扩展性能。支持高达 8～32 路处理器、64GB 内存、2～8 节点的集群。与 Windows Server 2003 Enterprise 版相比，该版本增加了一套 Windows Datacenter Program 程序包。这个产品同样增加了一个支持 64 位计算的版本。

1.1.3 Windows 网络管理任务

Windows Server 2003 网络管理的 5 个主要任务如下。

(1) Active Directory 管理。通常包括添加新的用户账户或更改现有账户的属性、委托管理、域控制器的管理等。

(2) 资源管理。用户经常访问的网络资源包括文件和打印机,常见的资源管理任务包括分配用户权限、配置打印机和将新的 Web 内容发布到 Web 服务器。

(3) 集中管理。应用组策略使管理员能够集中管理大量工作站和服务器。例如,一个策略可用于锁定桌面、编辑注册表、运行由 VBScript 编写的脚本程序或将网络上 200 台计算机的 My Document 文件夹重定向。另外,组策略还能用于集中部署和管理应用程序。

(4) 远程访问支持。如果用户经常在办公室外工作,或者需要从家中访问企业的网络资源,就必须通过拨号连接或虚拟专用网络连接方式来实现远程访问服务器。

(5) 网络支持。必须正确配置并维护支持 Active Directory、分布式文件系统(DFS)的基础网络服务,这些服务包括 DHCP、DNS、WINS 等。例如,由于办公室计算机数量的增加,需添加一个新的子网,此时就必须设置一个新的 DHCP 作用域来为新的计算机提供 IP 地址。

大型网络中的服务器已经进行了专门的分类,以满足客户不断增长的需求。大型网络中常见的服务器角色如下。

(1) 文件和打印服务器。

(2) 数据库服务器。

(3) 应用程序服务器(IIS、ASP.NET)。

(4) 邮件服务器(POP3、SMTP)。

(5) 终端服务器。

(6) 远程访问/VPN 服务器。

(7) 域控制器(Active Directory)。

(8) DNS 服务器。

(9) DHCP 服务器。

(10) 流式媒体服务器。

(11) WINS 服务器。

1.2 网络概述

1.2.1 TCP/IP

1. IP 地址

TCP/IP 网络上的每一台主机都分配有一个唯一的 IP 地址,以使这些主机在通信时

能够相互识别。

IP 地址共占用 4 个字节，每个字节称为一个 octet（八位位组），共计 32 位二进制数字。为了记忆和书写的方便，一般以 4 个十进制数表示，取值为 0～255，各 octet 之间用一个点号“.”分开（例如，192.168.10.1）。IP 地址由网络 ID 和主机 ID 两部分组成。网络 ID 表明主机所在的网络，每个网络都有唯一的网络 ID。主机 ID 标识了该网络上特定的某台主机，同一个网络内的每台主机都必须有唯一的主机 ID。

说明：此处所介绍的 IP 地址是目前广泛使用的 IPv4 地址，Windows Server 2003 还支持下一代的 IPv6 地址，它使用 128 位表示地址，因此可以提供更多数量的 IP 地址。

2. IP 地址的传统分类

IP 地址分为五类，即 A 类、B 类、C 类、D 类、E 类。其中只有 A 类、B 类、C 类 IP 地址可供一般主机使用。每类支持的 IP 地址数量不相同，以适应各种不同规模网络的需要。

如果以 W.X.Y.Z 的形式表示一个 IP 地址，即 W、X、Y、Z 分别表示 IP 地址的 4 个十进制数字，不同类别的 IP 地址其网络 ID 的位数与主机 ID 的位数不同，如表 1-1 所示。

表 1-1　IP 地址的传统分类

类 别	Network ID	Host ID	W 值的范围	支持的网络数	每个网络可支持的主机数
A 类	W	X.Y.Z	1～126	126	16 777 214
B 类	W.X	Y.Z	128～191	16 384	65 534
C 类	W.X.Y	Z	192～223	2 097 152	254

1）A 类地址

A 类地址适用于超大规模的网络。仅使用第一个 octet（8 位）表示网络 ID，后 3 个 octet（24 位）表示主机 ID。A 类地址的第一个 octet 的最高二进制位总为 0，这样就限制了 A 类地址第一个十进制数字的范围小于 127，因此仅有 127 个可能的 A 类网络。每一个 A 类网络能支持 16 777 214 个主机地址，这个数是由 $2^{24}-2$ 得到的。减 2 是必要的，因为全 0 的主机 ID 表示网络地址，而全 1 的主机 ID 表示网络广播地址。从技术上讲，127.0.0.0 也是一个 A 类地址，但是它已被保留作为环回（look back）测试之用而不能分配给一个网络，因此仅有 126 个 A 类网络。

2）B 类地址

B 类地址支持中到大型的网络。B 类 IP 地址使用前两个 octet（16 位）表示网络 ID，后两个 octet（16 位）表示主机 ID。B 类地址的第一个 octet 的最高两位总为 10，剩下的 6 位既可以是 0 也可以是 1，这样就限制了 B 类地址第一个十进制数字的范围介于 128～191 之间。B 类地址的后两个 octet（16 位）标识主机 ID。每一个 B 类网络能支持 64 534 个不同的主机地址，这个数由 $2^{16}-2$ 得到。B 类网络仅有 16 384 个。

3）C 类地址

C 类地址支持大量的小型网络。C 类地址使用前 3 个 octet（24 位）表示网络 ID，仅用最后一个 octet（8 位）表示主机 ID。C 类地址的第一个 octet 的前 3 位数为 110，这样就

限制了C类地址第一个十进制数字的范围介于192～223之间。每一个C类地址理论上可支持最大256个主机地址(0～255),但是仅有254个可用,因为0(全0主机ID)和255(全1主机ID)不是有效的主机地址。可以有2 097 152个不同的C类网络地址。

4) D类地址

D类地址用于在IP网络中的多播(multicasting)。D类地址的前4位总为1110,D类地址第一个十进制数字的范围介于224～239之间。

5) E类地址

E类地址留作研究之用,因此Internet上没有可用的E类地址。E类地址的前4位总为1,因此E类IP地址第一个十进制数字的范围介于240～255之间。

3. 子网掩码(Subnet Masks)

在TCP/IP中,子网掩码也是占用32位,用来区分网络上的主机是否在同一网络内。各类IP地址默认的子网掩码如表1-2所示。

表1-2 各类IP地址的默认子网掩码

类 别	默认的子网掩码(二进制)	默认的子网掩码(十进制)
A类	11111111 00000000 00000000 00000000	255.0.0.0
B类	11111111 11111111 00000000 00000000	255.255.0.0
C类	11111111 11111111 11111111 00000000	255.255.255.0

例如,如果A主机的IP地址为192.168.100.1,其二进制值为11000000.10101000.01100100.00000001,而子网掩码为255.255.255.0,其二进制值为11111111.11111111.11111111.00000000,则计算网络ID的方法如下。

(1) 将IP地址与子网掩码两个值中相应的二进制位进行逻辑与(AND)运算。

(2) 将逻辑与运算后的结果与子网掩码中的各字节互相映射,只要在子网掩码中位置为1的,其所映射的位就是网络ID。在IP地址中扣除网络ID后,其余的部分就是主机ID。

因此,A主机的网络ID就是192.168.100,用4个字节表示网络ID的话,其网络ID就是192.168.100.0,而主机ID就是1。同理,如果B主机的IP地址为192.168.100.5,子网掩码为255.255.255.0,则B主机的网络ID也是192.168.100.0。由于这两台主机的网络ID都是192.168.100.0,表示它们在同一个网络内,因此可以直接通信。反之,如果两台主机的网络ID不同,表示它们位于不同的网络内,因此无法直接沟通,必须通过路由器转发。

4. 默认网关

如果A主机要与位于同一个网络内的B主机通信,可以直接将数据发送给B主机;但是,如果要与位于不同网络的C主机通信,则必须将数据发送给路由器,再由路由器负责发送给C主机。一般来说,一台主机要通过路由器转发数据,必须将其"默认网关"指

向路由器的 IP 地址。

如图 1-1 所示，甲、乙两个网络利用路由器连接。

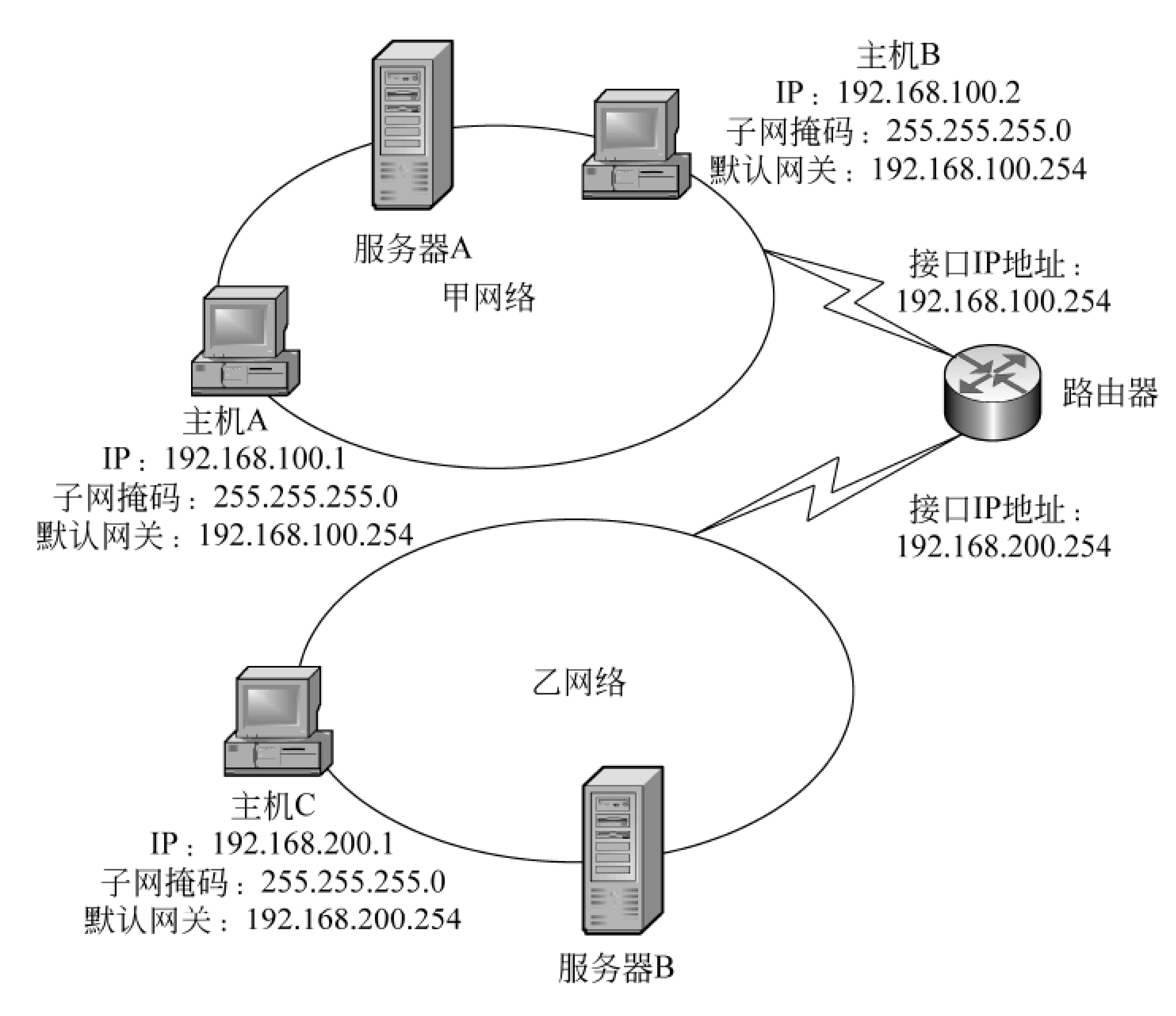


图 1-1　甲、乙两个网络通过路由器连接

如果甲网络上的主机 A 要与乙网络上的主机 C 通信，经过计算，主机 A 的网络 ID 为 192.168.100.0，而主机 C 的网络 ID 为 192.168.200.0，主机 A 和主机 C 位于不同的网络内，主机 A 会将数据发送给默认网关，也就是 IP 地址为 192.168.100.254 的路由器接口，然后由路由器转发给乙网络上的主机 C。

5. 专用 IP

专用 IP 也称为私有 IP(Private IP)，各公司可以自行选择适合的专用 IP，而且不需要申请，因此可以节省网络建设的成本。不过专用 IP 只能在公司内部的局域网使用，虽然它可以让内部计算机互通，但是无法与外部的网络(例如 Internet)直接通信。如果要与外部的网络互通，就必须通过网络地址转换(NAT)等途径解决。私有 IP 如表 1-3 所示。

表 1-3　私有 IP

类　别	专用 IP 范围
A	10.0.0.0～10.255.255.255，即 10.0.0.0/8
B	172.16.0.0～172.31.255.255，即 172.16.0.0/12
C	192.168.0.0～192.168.255.255，即 192.168.0.0/16

与专用 IP 对应的是公共 IP(Public IP)，例如 202.196.0.1。使用公用 IP 的计算机

可以直接和外部网络互通，因此可以在这些计算机上对外提供网络服务等，这些 IP 必须事先申请才能使用。

1.2.2 TCP/IP 实用工具

TCP/IP 协议集提供基本的 TCP/IP 实用工具，Windows 包括两类基于 TCP/IP 的实用工具：诊断工具和连接工具。

1. 诊断工具

允许用户检测和解决网络问题，常用的诊断工具命令如下。

(1) arp：显示和修改地址解析协议(ARP)高速缓存。

(2) hostname：显示计算机的主机名称。

(3) ipconfig：显示和更新当前的 TCP/IP 配置，包括 IP 地址。

(4) nbtstat：显示本地 NetBIOS 名称表。

(5) netstat：显示 TCP/IP 会话信息。

(6) ping：测试两台计算机之间的网络连接。

(7) tracert：跟踪数据包传送到目的地的路径。

2. 连接工具

允许通过不同的协议在计算机之间建立连接，常用的连接工具如下。

(1) FTP：使用 TCP 在客户端计算机和运行文件传输协议(FTP)的服务器之间传输文件。

(2) Telnet：远程访问运行 Telnet 服务的服务器。

(3) TFTP：使用 UDP 在客户端计算机和运行小型文件传输协议(TFTP)的服务器之间传输小型文件。

1.3 Windows 网络环境

根据网络中计算机的配置和访问信息的方式，Windows 支持工作组和域两种结构的网络。

1.3.1 工作组结构

工作组由一组用网络连接在一起的计算机组成，如图 1-2 所示。

工作组网络也称为对等网络，工作组结构的网络具有以下特征。

(1) 网络上每台计算机都有独立的本地安全账户数据库，称为安全账户管理器(Security Accounts Manager，SAM)数据库。如果一个用户要访问某台计算机内的资源，那么必须在这台计算机上(SAM 数据库内)为该用户创建用户账户。

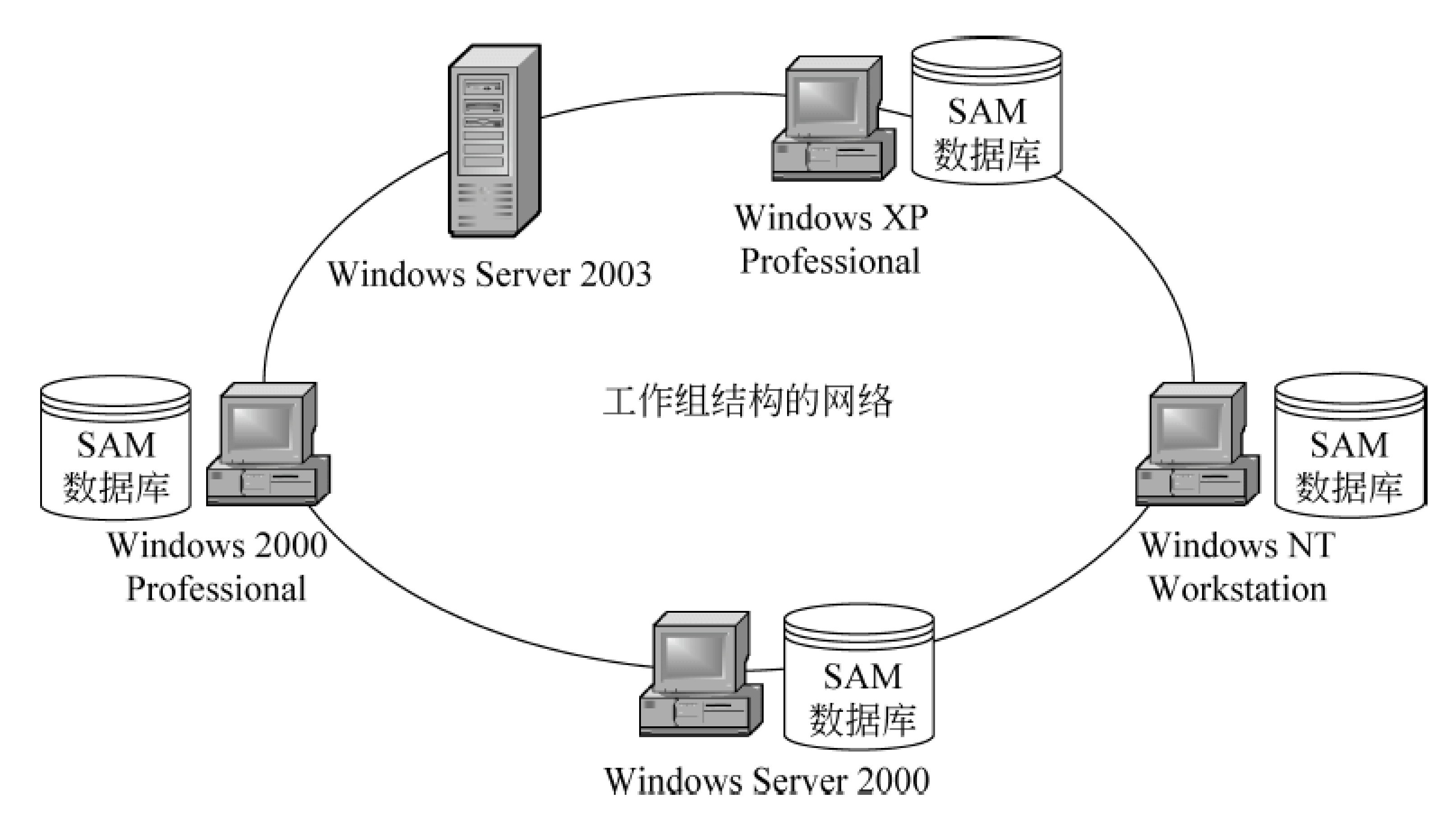


图 1-2　工作组结构的网络

（2）网络上没有专用的服务器，计算机间也不存在层次或隶属关系。所有计算机都是平等的，资源与管理分散在各个计算机上，不支持集中管理。

（3）用户数通常不超过 10 个。

（4）工作组中的计算机数量越多，越难管理。

1.3.2　域结构

域由一组用网络连接在一起的计算机组成，如图 1-3 所示。

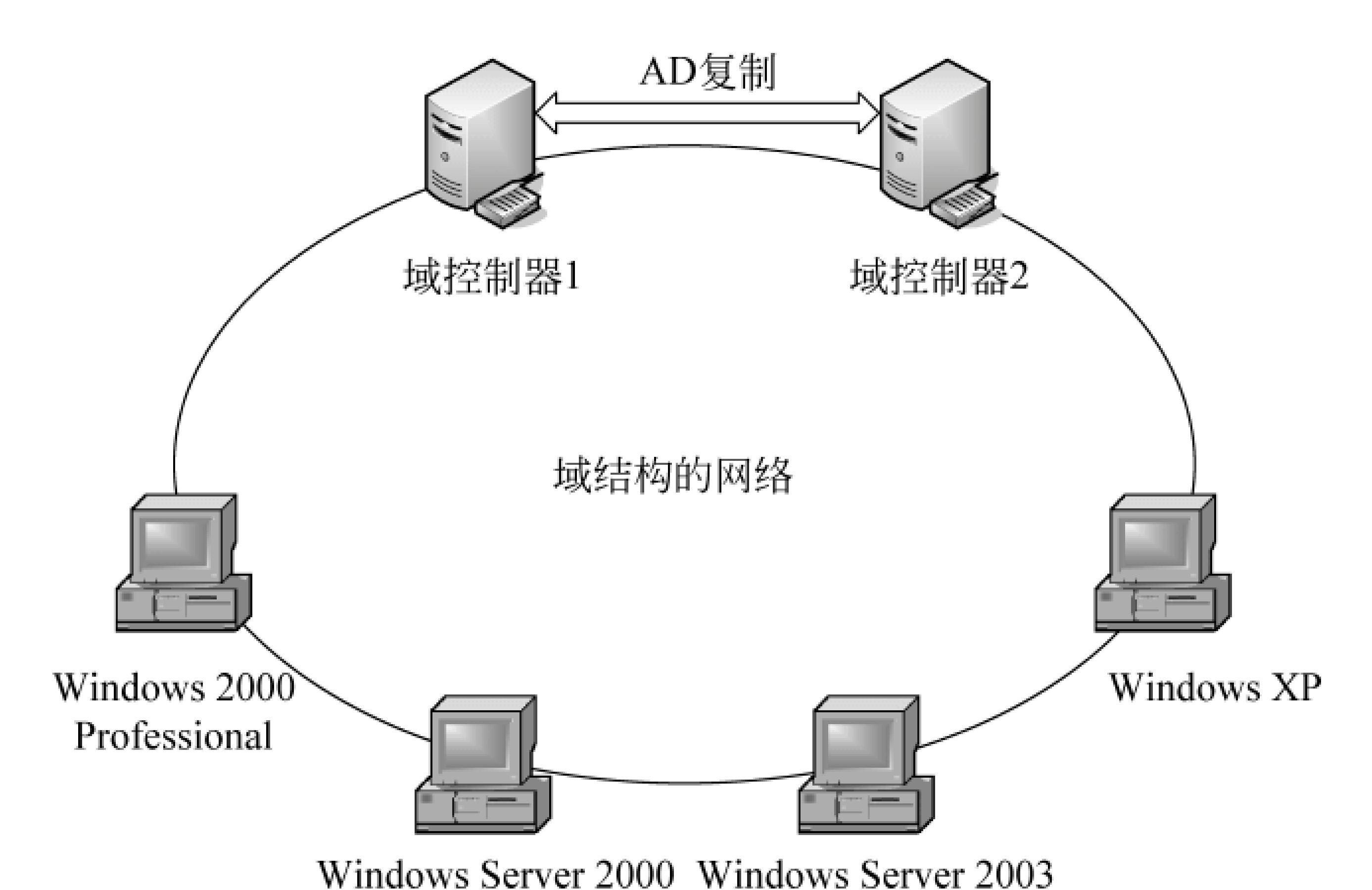


图 1-3　域结构的网络

域是网络上计算机的逻辑分组，域结构的网络具有以下特征。

（1）集中式的资源、管理和认证。

（2）域中所有的计算机共享一个集中式的目录数据库，它包含了整个域内的用户账户与计算机账户信息。

(3) 用户只需要有一个域用户账户就能访问域中的共享资源。

(4) 支持的计算机数量可从数台到数千台。

域提供了集中管理网络资源的方法,如下所述。

(1) 单一登录。域为用户提供了一次单独登录的流程以便访问各种网络资源,包括文件、打印和应用程序资源。所有的用户账户都存储在一个集中位置。

(2) 单一用户账户。域里的用户只需要一个单一的账户就可以访问各台计算机上的资源。而工作组里的用户在每台他们需要访问的计算机上都需要一个单独的账户。

(3) 集中化管理。域提供了集中化管理。所有的用户账户和资源的信息都可以在域里的某个位置统一管理。

(4) 可伸缩性。域可以扩展为更大规模的网络。在大规模网络上,用户访问资源的方式和资源管理的方式与小规模网络相同。

1.4 配置 Windows 网络

1.4.1 安装与设置 TCP/IP

在 Windows Server 2003 中默认已经安装了 TCP/IP。如果没有安装,可以打开“控制面板”,双击“网络连接”,右击后选择“本地连接”→“属性”→“安装”→“协议”→TCP/IP,即可开始安装 TCP/IP。

如果要对 TCP/IP 进行设置,操作步骤为:打开“网上邻居”,右击后选择“本地连接”→“属性”→“Internet 协议(TCP/IP)”选项,出现如图 1-4 所示的对话框后,可以修改 TCP/IP 设置。

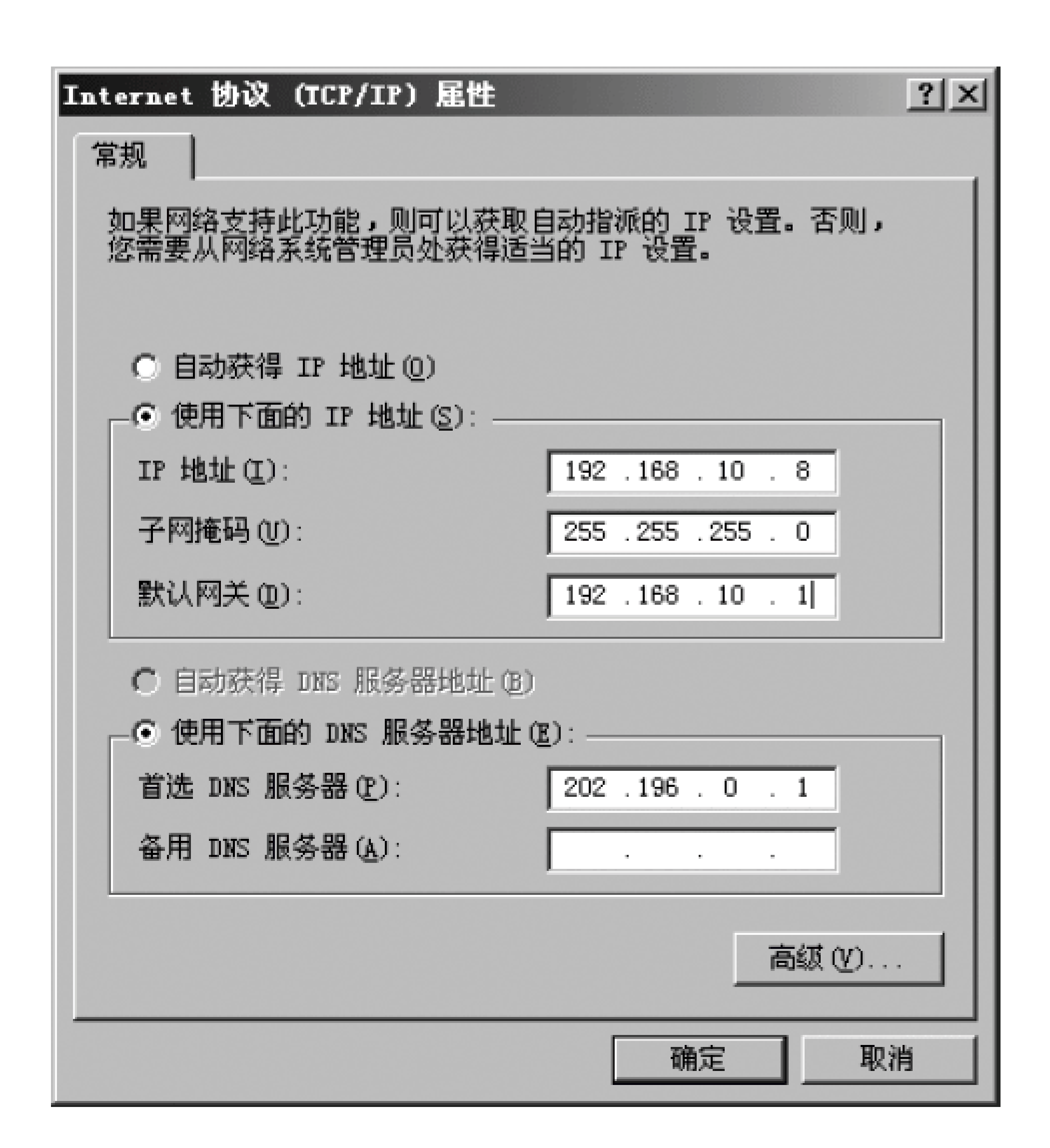


图 1-4 Internet 协议(TCP/IP)属性

如果用户设置的新 IP 地址与其他计算机重复，会出现如图 1-5 所示的提示信息。

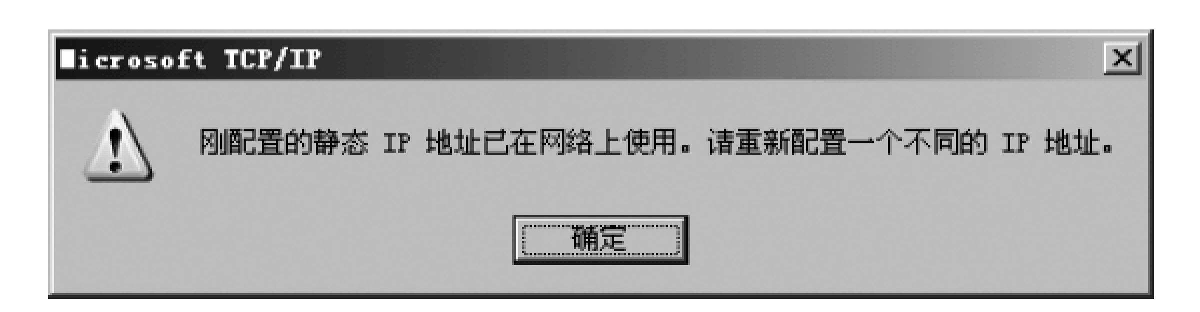


图 1-5　IP 地址冲突

完成后，在“命令提示符”下利用 ipconfig 与 ping 命令检查设置是否正确，如图 1-6 和图 1-7 所示。

```
命令提示符
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接 2:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.10.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1

C:\Documents and Settings\Administrator>
```

图 1-6　ipconfig 命令

```
命令提示符
C:\Documents and Settings\Administrator>ping 192.168.10.8

Pinging 192.168.10.8 with 32 bytes of data:

Reply from 192.168.10.8: bytes=32 time=2ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

图 1-7　ping 命令

1.4.2　配置 Windows 防火墙

Windows Server 2003 从 Service Pack 1 开始增加了“Windows 防火墙”功能，自带的防火墙工具是 Internet 连接防火墙(Internet Connection Firewall，ICF)，以便保护计算机免受外部攻击。

要启用 Windows 防火墙，可以双击“控制面板”中的“Windows 防火墙”，在如图 1-8 所示的对话框中选择“启用”即可。启动“Windows 防火墙”后，它就会阻挡未授权用户通过网络访问此计算机。

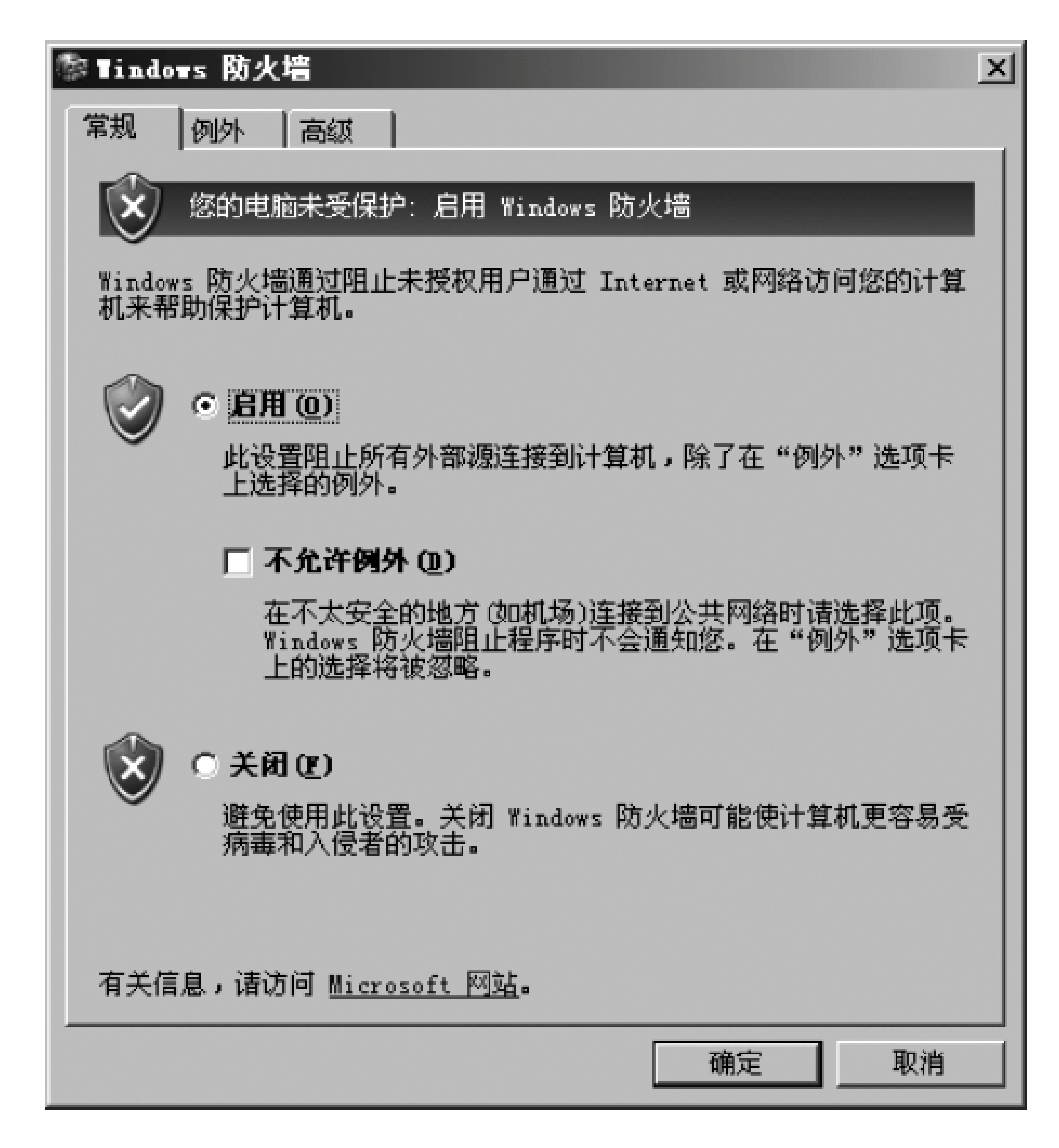


图 1-8 Windows 防火墙

可以通过“例外”选项卡来开放部分资源，例如开放文件和打印机共享、远程桌面、UPnP 框架等，如图 1-9 所示。



图 1-9 Windows 防火墙的“例外”选项卡

如果要开放端口，请单击“添加端口”按钮，输入名称与端口号，如图 1-10 所示。

如果要开放程序，请单击“添加程序”按钮，选择列表中现有的程序，或单击“浏览”按钮选择未列出的程序，如图 1-11 所示。

添加端口
使用这些设置打开通过 Windows 防火墙的端口以使用。要查找端口号和协议，请查阅您要使用的程序或服务的文档。
名称(N):
端口号(P):
TCP(T)　UDP(U)
更改范围(C)...　确定　取消

图 1-10 “添加端口”对话框



图 1-11 “添加程序”对话框

如果用户不允许例外，也就是说要阻挡外部来的所有访问行为，请选中“不允许例外”复选框。

1. 设置常规网络服务

默认情况下，ICF 提供了 WWW、FTP 等常用网络服务的防火墙设置。单击图 1-8 中的“高级”选项卡，如图 1-12 所示。

单击“设置”按钮，进入“高级设置”对话框。在“服务”选项卡中，提供了常用网络服务的列表。例如，如果需要提供 FTP 服务，则只需勾选“FTP 服务器”选项，如图 1-13 所示。在打开的“服务设置”对话框中保持默认的计算机名即可。

2. 设置非常规服务

为了防止用户的非授权访问，经常需要将一些常规网络服务的默认端口屏蔽掉，而采用一些非默认端口提供常规的网络服务。例如，可以使用 8080 端口提供 WWW 服务。单击图 1-13 中的“添加”按钮，打开“服务设置”对话框。在该对话框中添加相应信息，注意一定要在外部和内部端口号中添加 8080，如图 1-14 所示，然后单击“确定”按钮。这时

即可在服务列表中看到刚刚添加的服务。



图 1-12　Windows 防火墙的“高级”选项卡



图 1-13　允许 FTP 服务

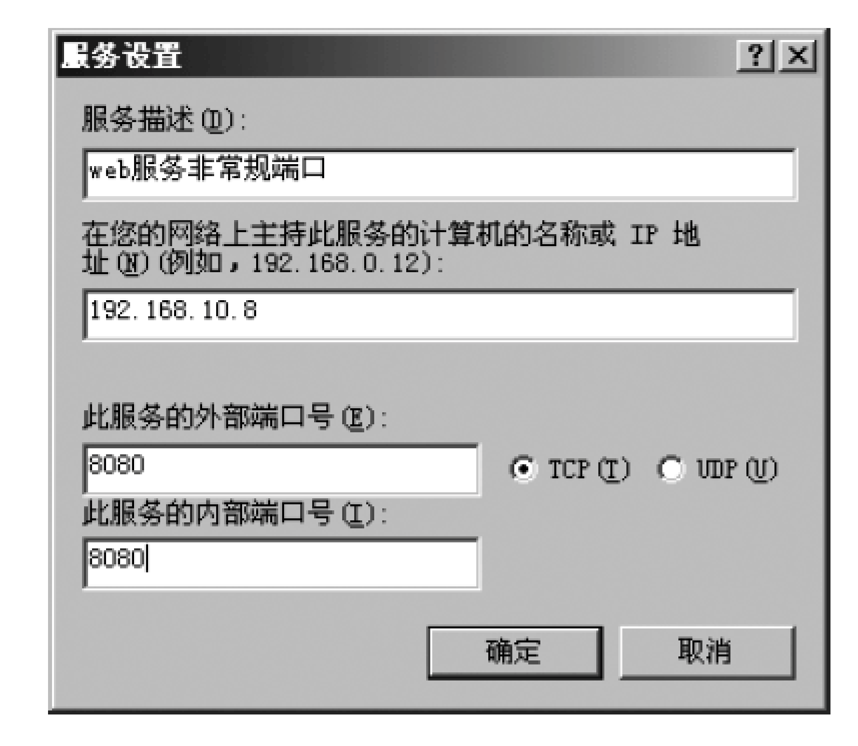


图 1-14　“服务设置”对话框

3. ICMP 设置

ICMP 即 Internet 控制信息协议，最常用的 ping 命令就是基于 ICMP 的。默认情况下，ICF 禁用了应用该协议的信息请求，例如，不允许 ping 本机。如果由于特殊需要而想 ping 本机，则需要在图 1-13 所示的对话框中单击 ICMP 选项卡，在打开的选项卡中勾选“允许传入响应请求”选项，如图 1-15 所示。

4. 设置安全日志

设置安全日志可以使服务器在受到恶意攻击后保留安全日志。单击图1-12"安全日志记录"中的"设置"按钮,在"日志设置"对话框中勾选"记录被丢弃的数据包"和"记录成功的连接"两个复选框。这样就可以通过查看相应目录中保存的日志文件了解来访者的信息,如图1-16所示。

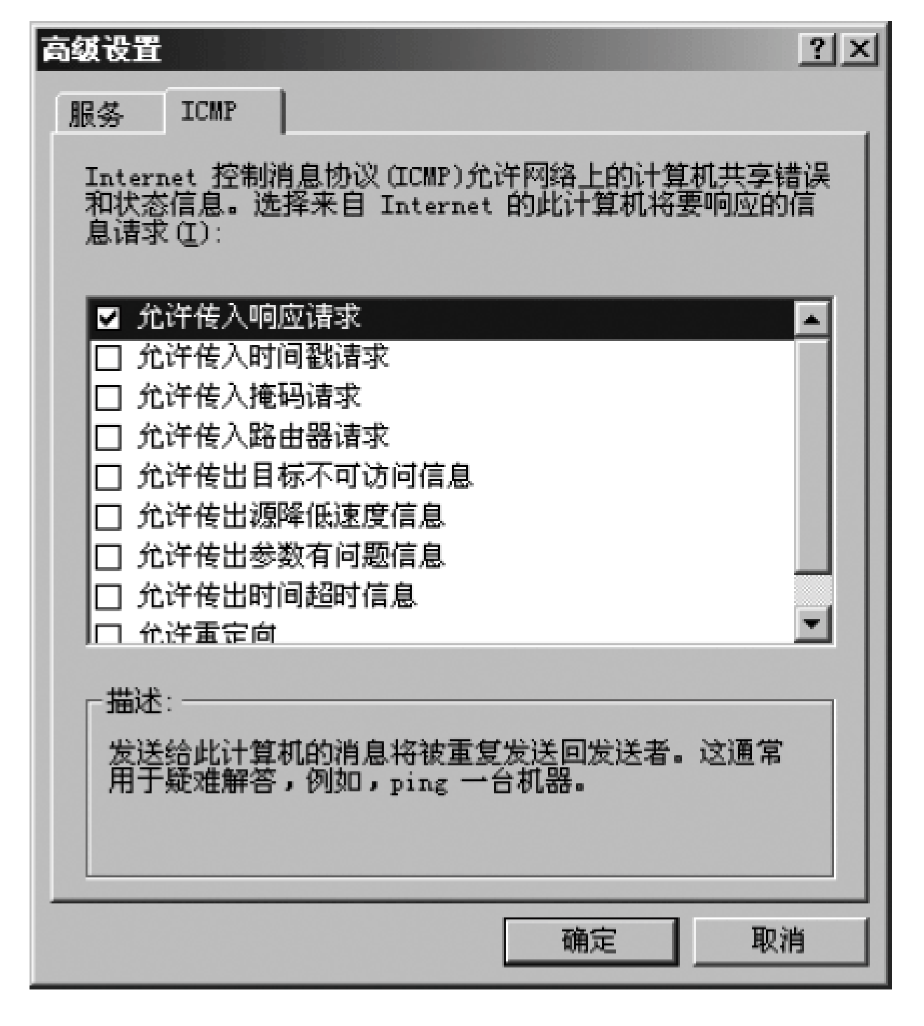


图1-15 ICMP允许传入响应请求



图1-16 Windows防火墙日志设置

ICF可以有效拦截某些用户对服务器的扫描和攻击,并且可以有效防范利用系统漏洞进行端口攻击的蠕虫病毒(如冲击波等)。无论对于个人计算机还是网络服务器,都可以起到很好的保护作用。

第 2 章　NTFS 文件系统

学习目标

学习完本章后，能够掌握 NTFS 文件系统、NTFS 权限设置、共享文件夹及其权限设置、共享文件夹的设置与访问。

2.1　NTFS 概述

NTFS(NT File System)是 Windows Server 2003 所支持的一种文件系统。NTFS 具有如下优点。

(1) 提供了安全性，允许基于文件分配权限。

(2) 优化了文件系统的结构、簇尺寸、磁盘碎片、文件数等。

(3) 支持文件压缩，以节省磁盘空间。

(4) 支持文件加密，以增强数据的安全性。

(5) 支持磁盘配额功能，可以让管理员管理用户使用磁盘的空间。

(6) 域与活动目录的使用，使得管理与使用网络资源更为容易。

(7) 可以审核文件资源的使用并可以跟踪用户访问文件的情况。

(8) NTFS 文件系统支持 Unicode 统一编码，可以解决不同语言系统间的兼容性问题。

2.2　NTFS 权限应用

当用户试图访问文件或者文件夹时，NTFS 文件系统会检查用户使用的账户或者账户所属的组是否在此文件或者文件夹的访问控制列表(ACL)中，如果存在则进一步检查访问控制项(ACE)，然后根据控制项中的权限来判断用户最终的权限。如果访问控制列表中不存在用户使用的账户或者账户所属的组就拒绝用户访问。

Windows Server 2003 中的标准权限如图 2-1 所示。

标准权限包括如下。

(1) 完全控制：对文件或者文件夹可执行所有操作。

(2) 修改：可以修改、删除文件或者文件夹。

(3) 读取和运行：可以读取内容，并且可以执行应用程序。

(4) 列出文件夹目录：可以列出文件夹内容，此权限只针对文件夹。

(5) 读取：可以读取文件或者文件夹的内容。

(6) 写入：可以创建文件或者文件夹。

(7) 特别的权限：其他不常用权限，比如删除权限。

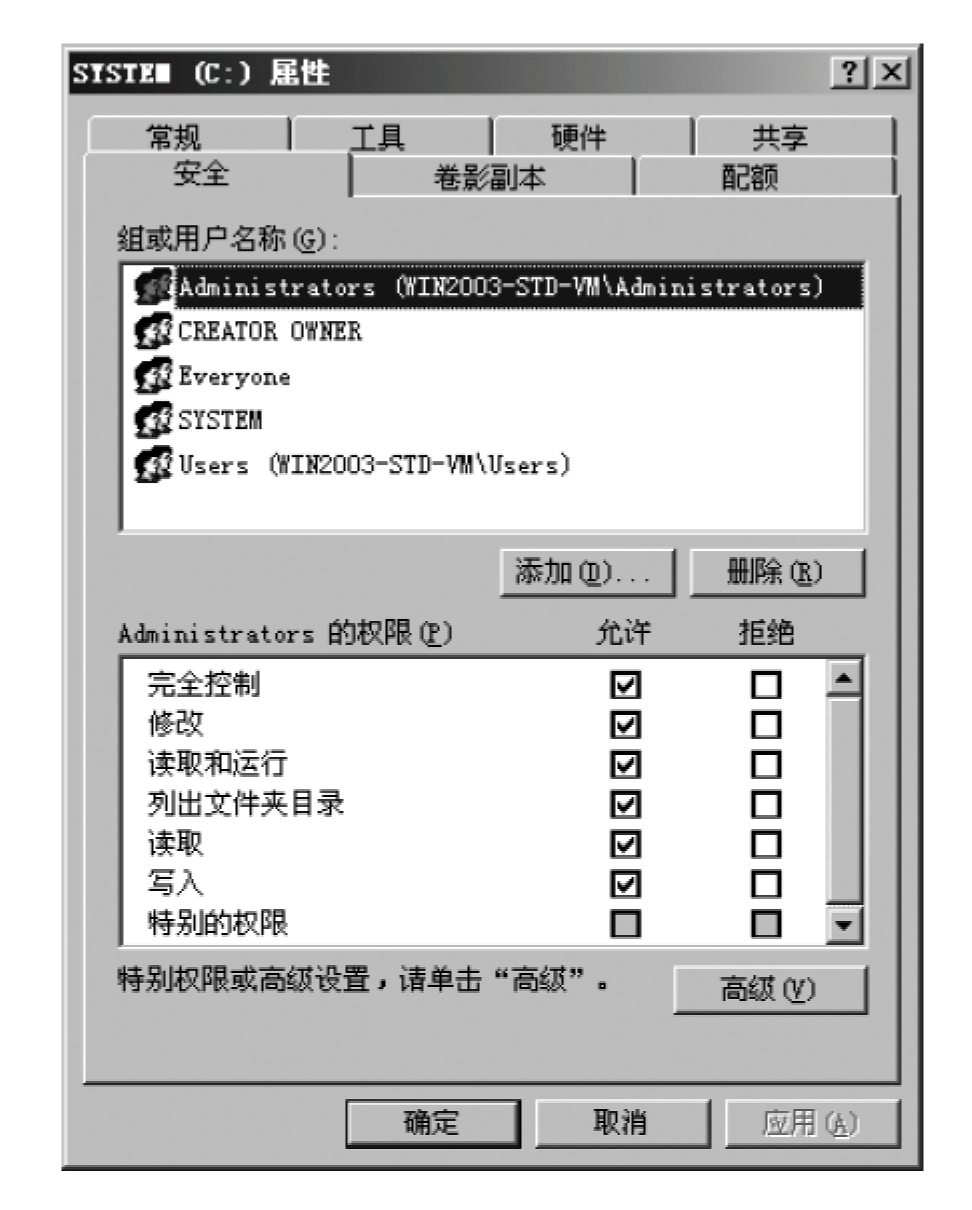


图 2-1 NTFS 权限

2.2.1 多重 NTFS 权限的规则

在应用多重 NTFS 权限时，需要注意的规则如下。

1. 权限的累积

用户对资源的有效权限是分配给该用户账户和用户所属的组的所有权限的总和。如果用户对文件具有“读取”权限，该用户所属的组又对该文件具有“写入”的权限，那么该用户就对该文件同时具有“读取”和“写入”的权限。

2. 文件权限高于文件夹权限

NTFS 文件权限对于 NTFS 文件夹权限具有优先权，如果用户能够访问一个文件，那么即使该文件位于用户不具有访问权限的文件夹中，也可以进行访问（前提是该文件没有继承它所属的文件夹的权限）。

3. 拒绝高于其他权限

拒绝权限可以覆盖所有其他的权限。甚至作为一个组的成员有权访问文件夹或文件，但是该组被拒绝访问，那么该用户本来具有的所有权限都会被锁定而导致无法访问该文件夹或文件，也就是说上面第一点的权限累积原则将失效。

2.2.2 NTFS 权限的继承性

NTFS 权限具有继承性。默认情况下，授予父文件夹的权限将被该父文件夹下的子文件夹或文件所继承。也就是说文件或文件夹默认会继承分区或父文件夹的权限，并且继承来的权限不能直接设置和修改，只能在此基础上添加其他权限。

利用 Administrators 账户登录，在 C 盘下新建 test 文件夹。然后查看其属性，如图 2-2 所示。

为 Guest 用户添加“读取和运行”、“列出文件夹目录 ”、“读取”权限，如图 2-3 所示。



图 2-2 test 文件夹权限

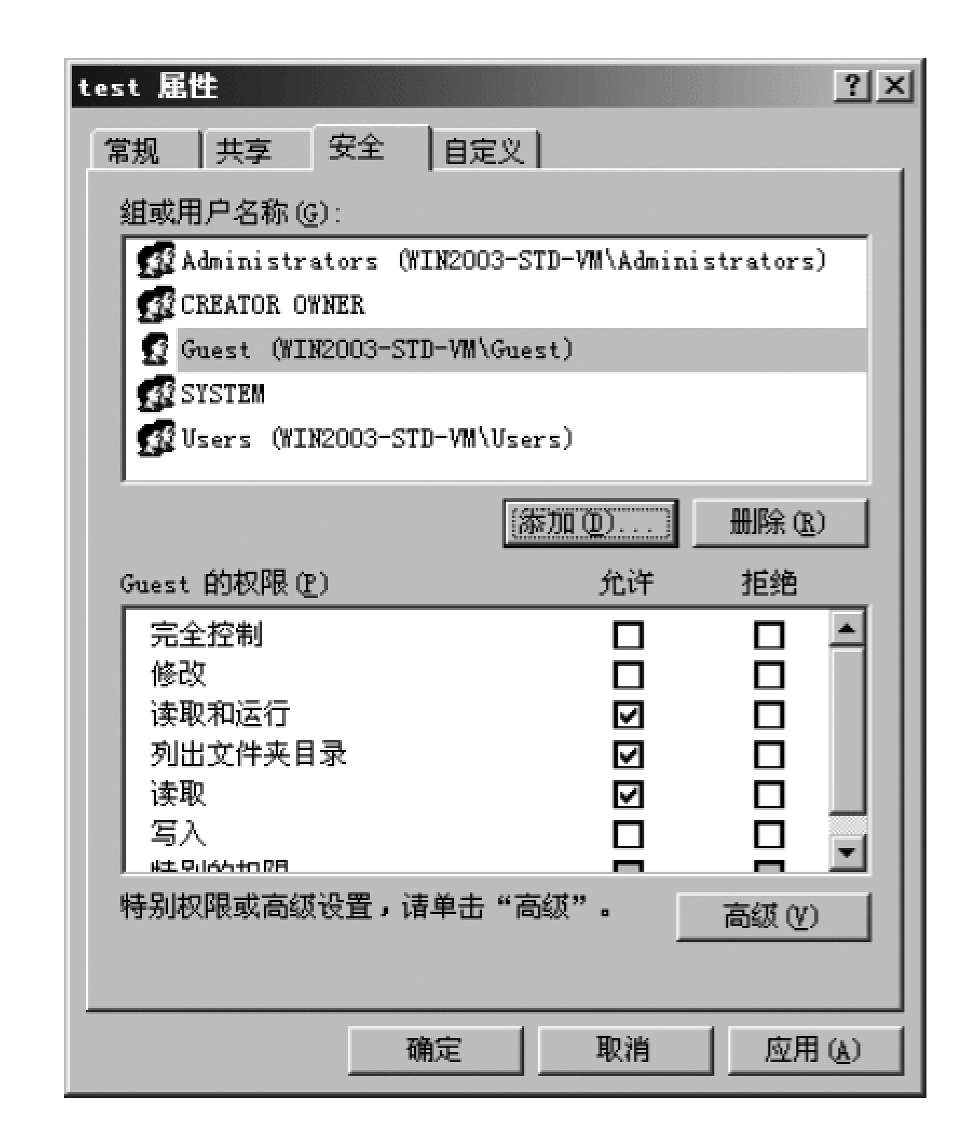


图 2-3 父文件夹权限

在 C:\test 文件夹下新建 test1 文件夹，发现 test1 文件夹继承了 C:\test 的权限，灰色对号表示这些权限是继承的，并且不能直接设置和修改，只能在此基础上添加其他权限，如图 2-4 所示。

需要说明的是，NTFS 权限在移动和复制文件时的继承性，同一个 NTFS 分区内或不同 NTFS 分区之间移动或复制一个文件或文件夹时，该文件或文件夹的 NTFS 权限会发生不同的变化。

(1) 在同一个 NTFS 分区内移动文件或文件夹时，其实质就是在目的位置将原位置上的文件或文件夹“搬”过来，因此文件和文件夹仍然保留有在原位置的一切 NTFS 权限。

(2) 在不同 NTFS 分区之间移动文件或文件夹时，文件和文件夹会继承目的分区中文件夹的权限，其实质就是在原位置删除该文件或文件夹，并且在目的位置新建该文件或文件夹。

(3) 在同一个 NTFS 分区内复制文件或文件夹时，复制文件和文件夹将继承目的位



图 2-4　子文件夹权限

置中的文件夹的权限。

(4) 在不同 NTFS 分区之间复制文件或文件夹时，复制文件和文件夹将继承目的位置中的文件夹的权限。

2.2.3　设置 NTFS 权限

要为 Guest 用户设置不同的访问权限，操作步骤如下。

(1) 在 NTFS 磁盘分区创建一个 test 文件夹，在该文件夹下面分别创建 test1 和 test2 文件夹。这两个文件夹默认都继承了父文件夹的访问权限。

(2) 右击 test1 文件夹，在弹出的菜单中选择“共享和安全”，或者在右键菜单中选择“属性”，在弹出的文件夹的属性窗口中选择“安全”选项卡。可以看出，test1 文件夹继承了 test 文件夹的访问权限，并且不能直接修改。

(3) 单击“高级”按钮，弹出如图 2-5 所示的“高级安全设置”对话框。

在图 2-5 中，有两个复选框，分别如下。

① “允许父项的继承权限传播到该对象和所有子对象，包括那些在此明确定义的项目”复选框表示要继承父项的权限设置。

② “用在此显示的可以应用到子对象的项目替代所有子对象的权限项目”复选框表示以该文件夹的权限替代该文件夹内子对象的权限。

明确了以上两个复选框的意义之后，对于 test1 文件夹，选中“允许父项的继承权限传播到该对象和所有子对象，包括那些在此明确定义的项目”复选框，这样就可以更改权限，弹出如图 2-6 所示的信息提示框。

在图 2-6 中有两个按钮，分别是“复制”和“删除”。

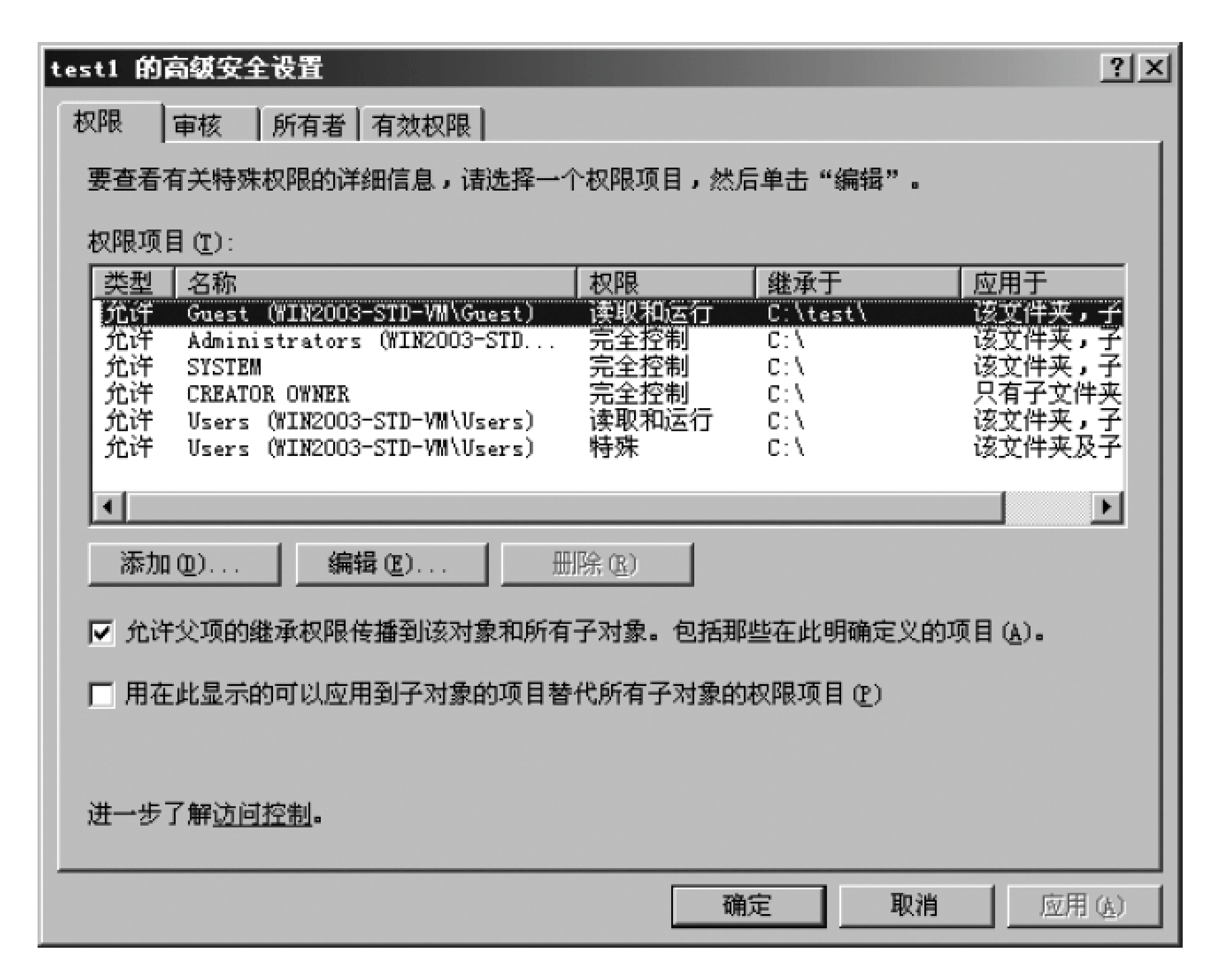


图 2-5　test1 的高级安全设置

① “复制”按钮表示将现有的从父文件夹继承来的权限复制一份，保留给该文件或文件夹，然后断开继承关系，同时也可以修改继承来的权限或者再分配权限。

② “删除”按钮表示将从父文件夹继承来的所有权限彻底删除，然后断开继承关系。

单击“复制”按钮，可以看到 Guest 用户对于 test1 的权限，如图 2-7 所示。

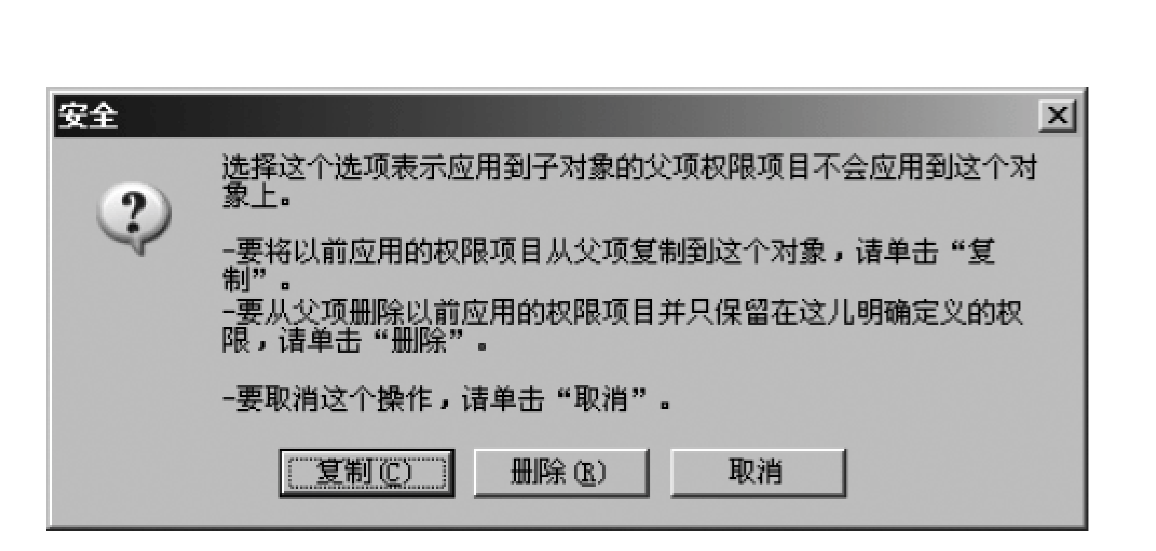


图 2-6　信息提示框

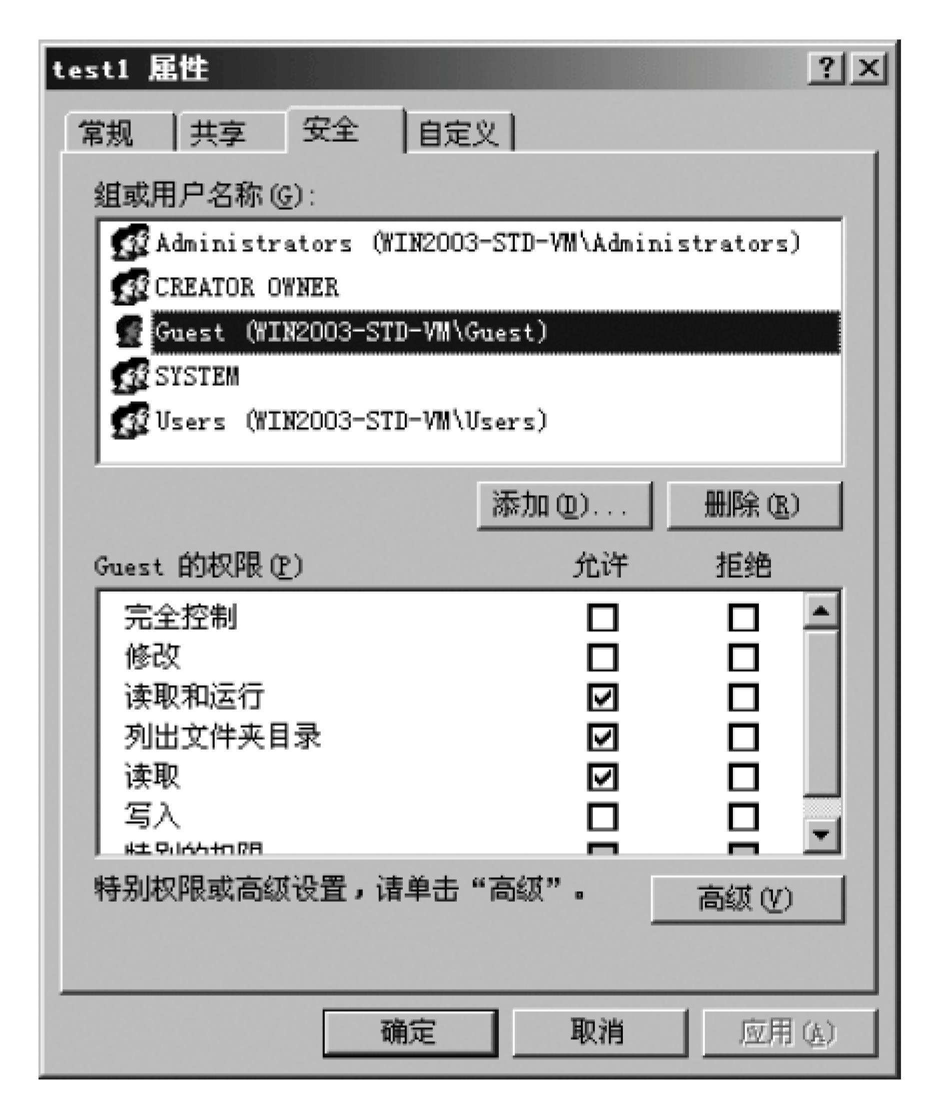


图 2-7　更改后的 test1 文件夹属性

对 test2 文件夹，选择删除，会将所有的账户权限都删除。然后新建 Guest 账户的权限，如图 2-8 所示。

对 test2 文件夹的权限设置的结果，如图 2-9 所示。

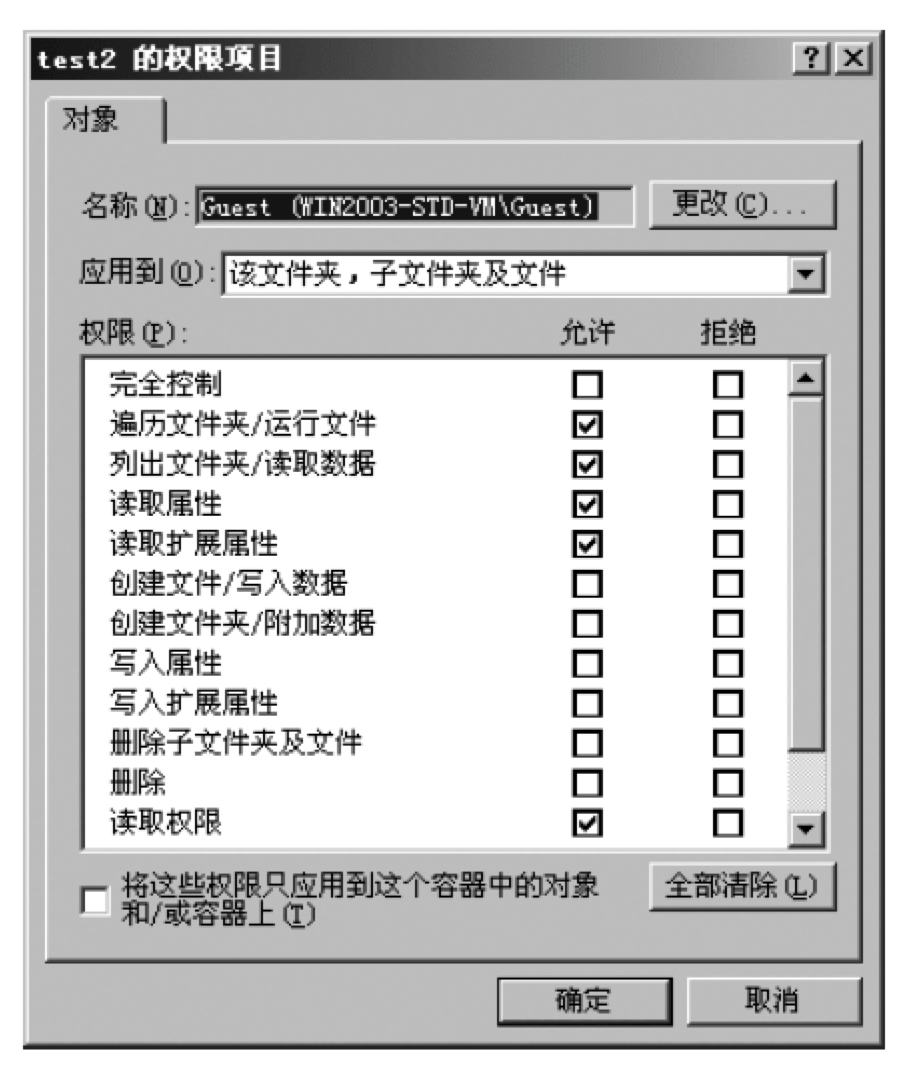


图 2-8　test2 文件夹高级安全设置

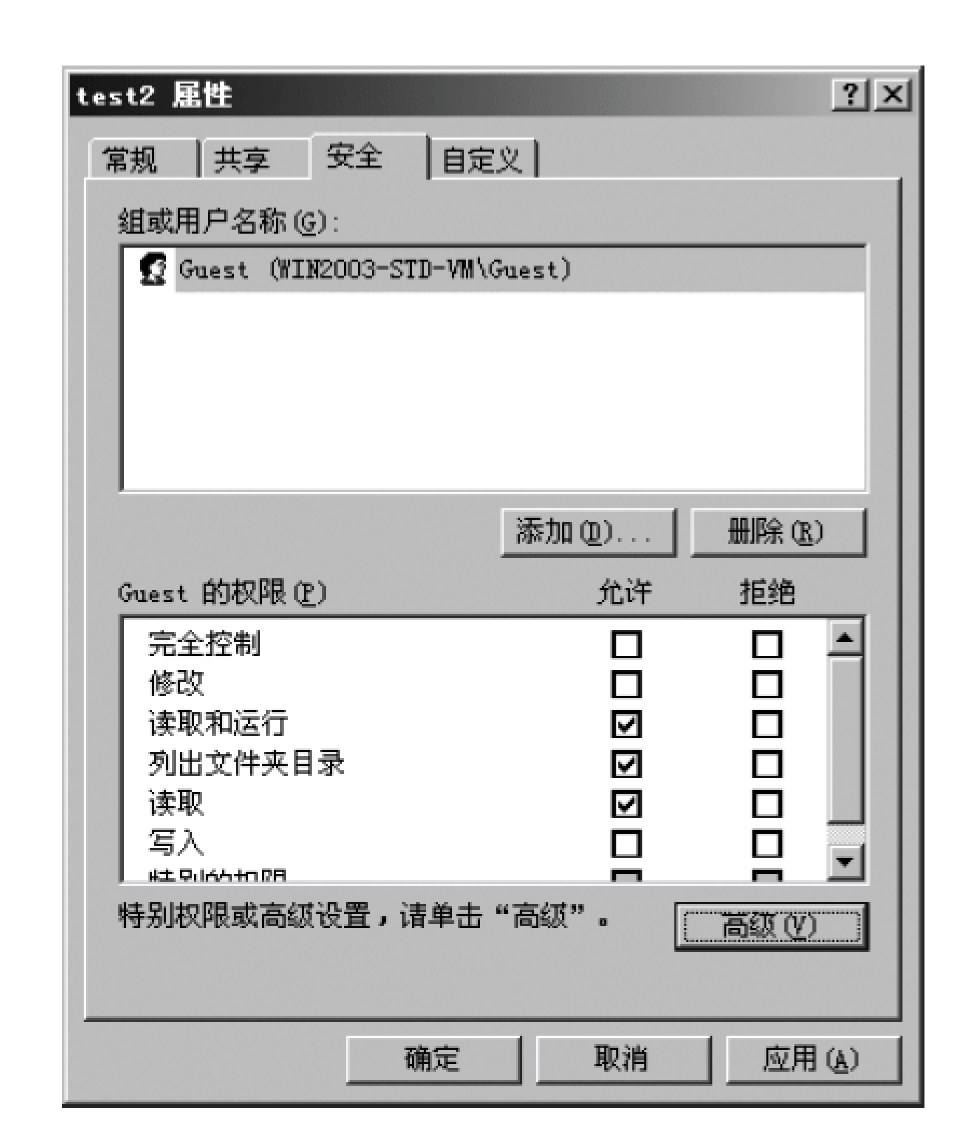


图 2-9　更改后的 test2 文件夹属性

2.3　共享文件夹

要让局域网上的其他用户通过网络访问服务器上的某个文件夹，可以将这个文件夹设置为“共享文件夹”。共享文件夹不受文件系统的限制，即 NTFS、FAT、FAT32 分区内的文件夹，都可以被设置为共享文件夹。

2.3.1　设置共享文件夹

用户必须属于 Administrators、Server Operators、Power Users 等内置组的成员，才有权利将文件夹设为共享文件夹。

要把一个文件夹设置为共享文件夹，操作步骤为：右击文件夹，然后选择“属性”，就会出现属性对话框，单击“共享”选项卡，如图 2-10 所示。

选中“共享此文件夹”单选按钮，即可将此文件夹共享，还可以进行其他设置，如图 2-11 所示。

(1) 共享名。共享名默认与文件夹的名称相同，用户可以自行修改该名称。网络上的用户就是通过该共享名来访问文件夹的内容。

(2) 注释。如果需要的话，可以在此处输入一些说明文字。

(3) 用户数限制。用户可以在此处限制一次最多可以有多少个用户与该共享文件夹连接。默认为“最多用户”，也就是没有限制。

(4) 权限。默认是所有用户都有读取共享文件夹的权限，如果要更改，请单击“权限”按钮，其操作说明与 NTFS 权限设置类似。

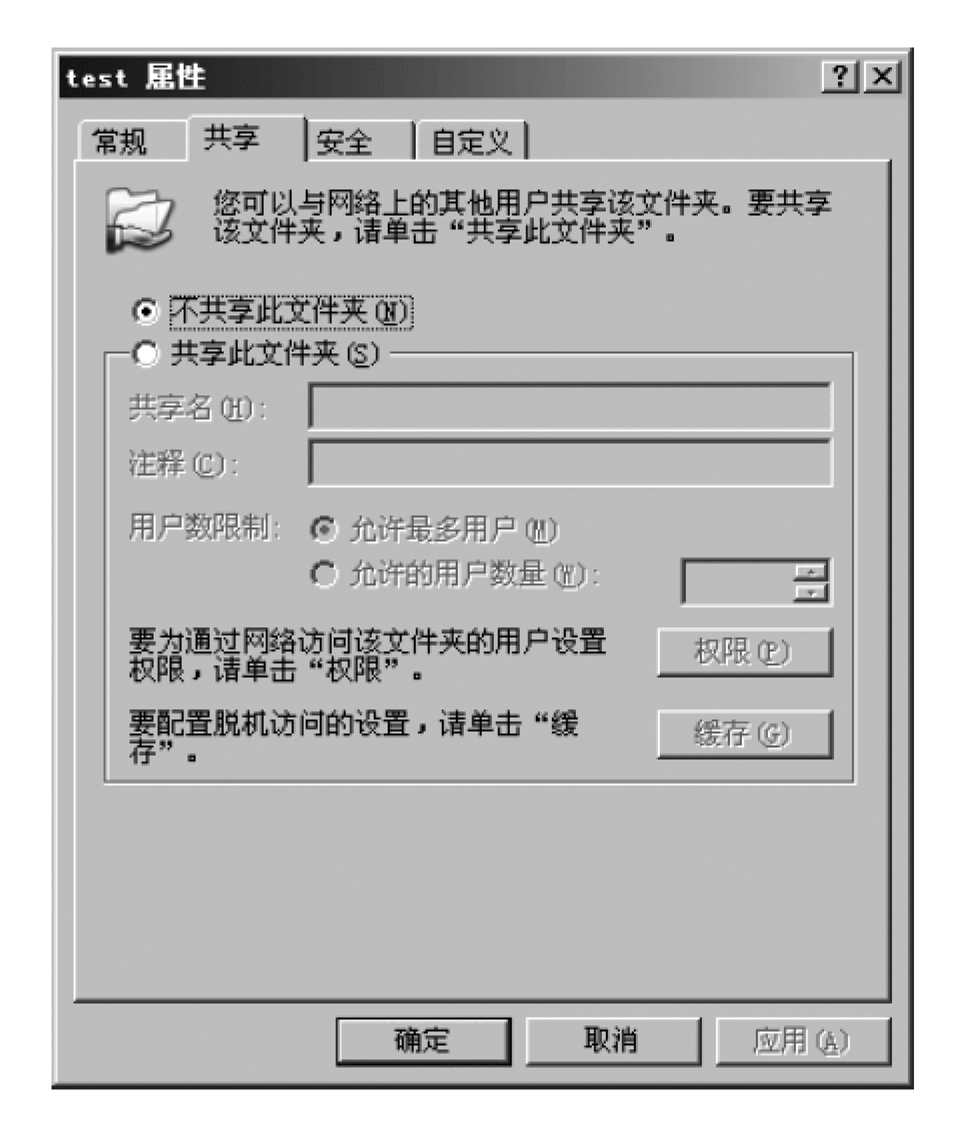



图 2-10 "共享"选项卡

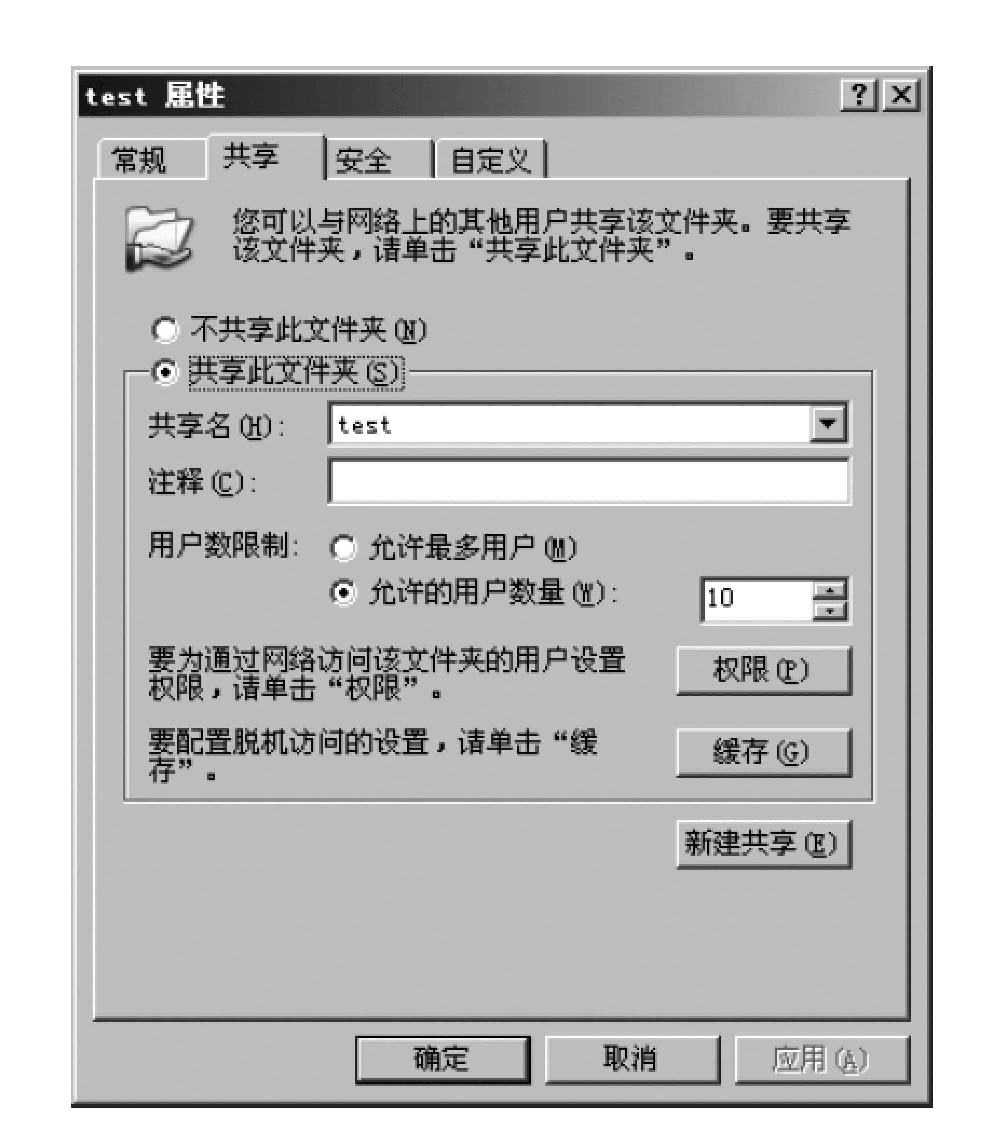


图 2-11 共享选项卡设置

(5) 缓存。用于设置如何让用户在脱机时访问该共享文件夹。

(6) 新建共享。用于给一个文件夹设置多个共享名，只需要单击"新建共享"按钮后输入新的共享名及其相关的设置即可(注意，只有在此文件夹是共享文件夹的前提下才会出现"新建共享"按钮)。设置完成后，可以看到文件夹上出现了共享标志。

如果要终止共享该文件夹，则只要选择"不共享此文件夹"单选按钮即可。

2.3.2 客户端如何访问共享文件夹

网络上的用户可以利用以下 4 种方式访问共享文件夹中的文件。

1. 自动搜索共享文件夹

Windows Server 2003 计算机具备自动在网络上查找共享文件夹的功能，对于其他系统，可以打开"我的电脑"中的"工具"菜单中的"文件夹选项"，选中"查看"选项卡，然后选中如图 2-12 所示的选项。

设置后，在"网上邻居"中，用户可以看到共享文件并直接通过该窗口访问这些共享文件夹。需要注意的是，系统只会自动帮助用户在网络上查找该用户有权访问的共享文件夹。

2. 利用"网上邻居"

以 Windows Server 2003 为例，可以通过"网上邻居"中的"搜索"工具来搜索特定 IP 地址的计算机，如图 2-13 所示，然后可以打开共享文件夹。

如果之前用户登录到计算机时输入的用户账户没有权利连接该计算机，则系统会重

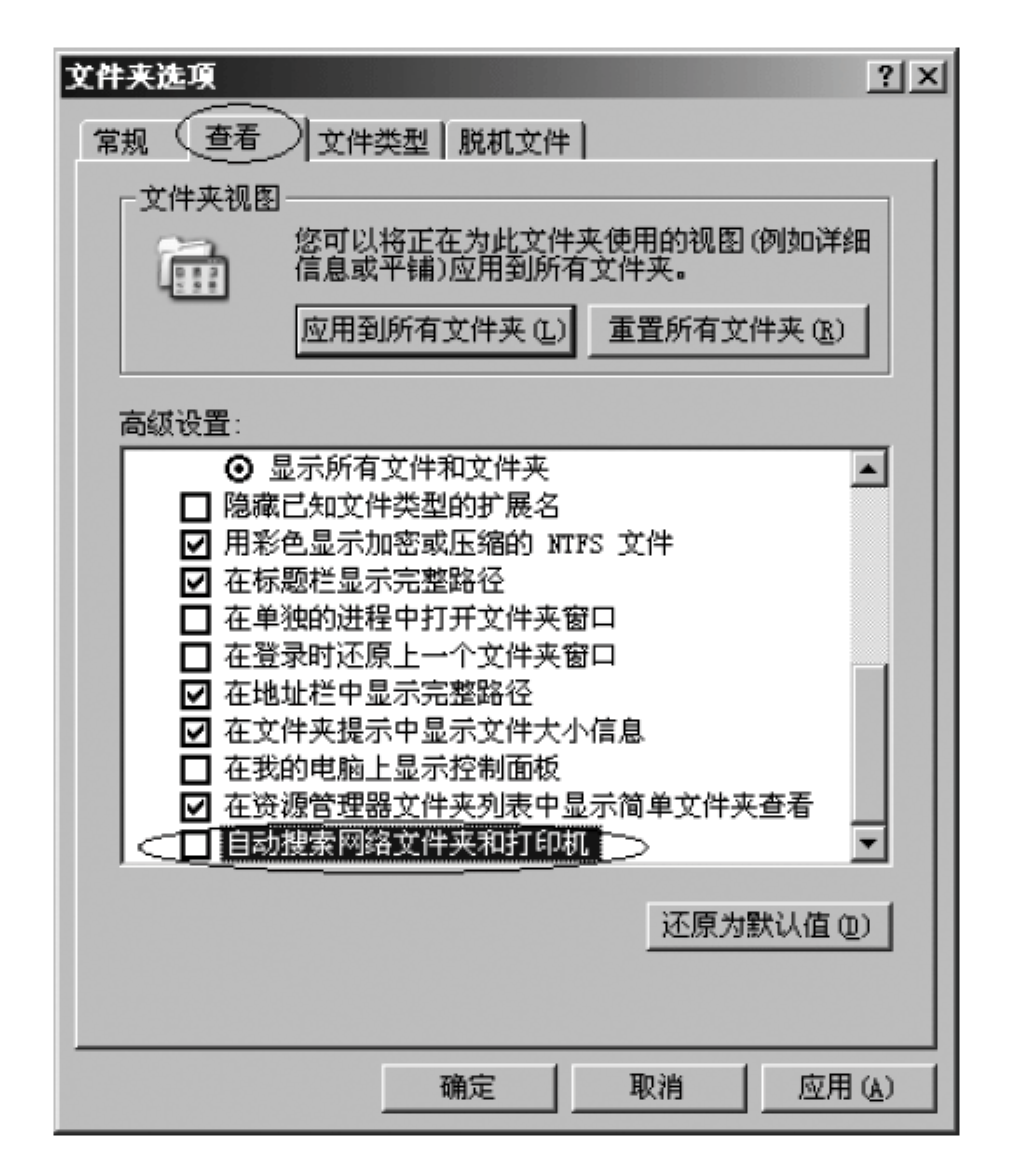


图 2-12　自动搜索网络文件夹和打印机选项

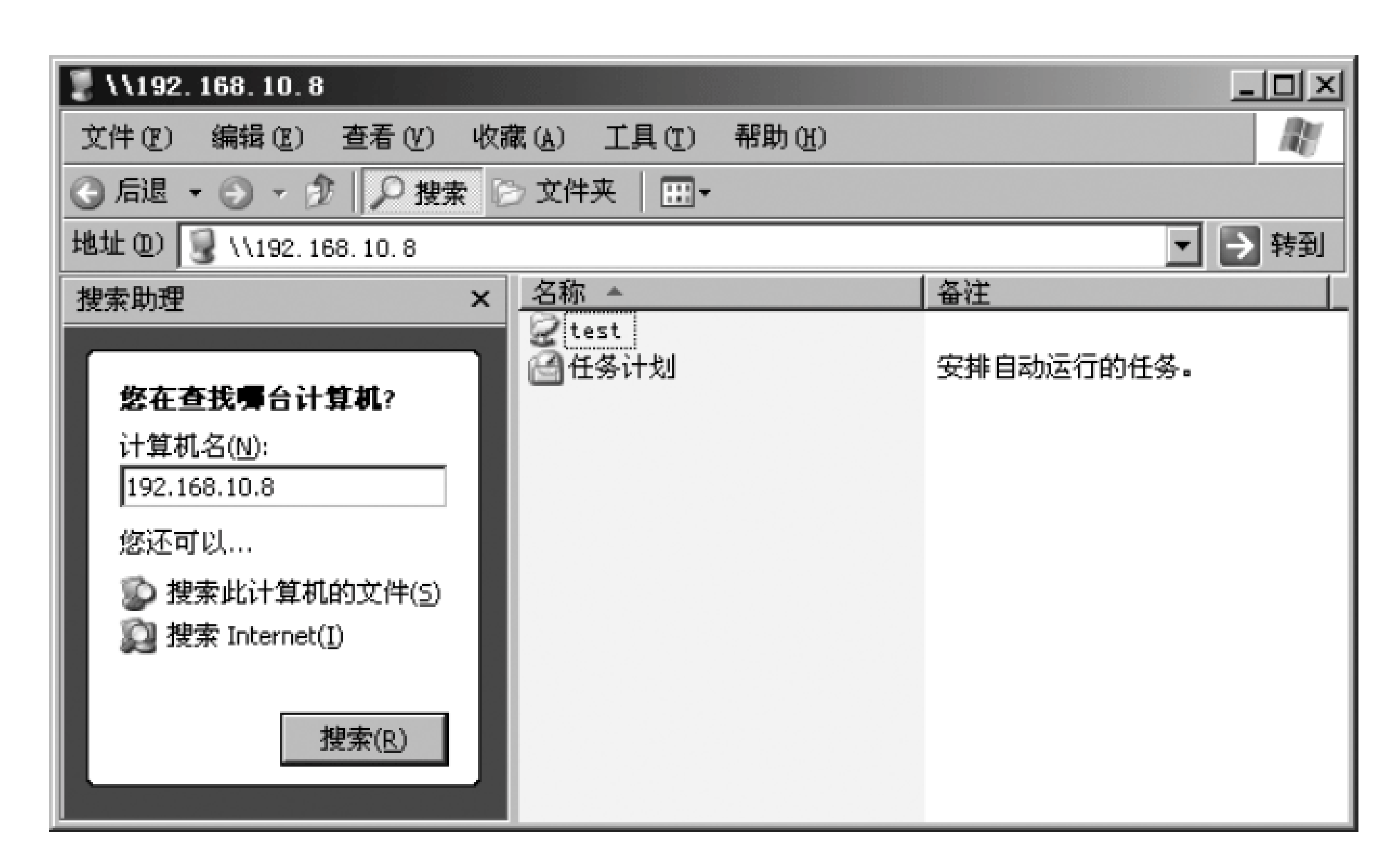


图 2-13　网上邻居中的搜索命令

新要求用户输入该计算机内有效的用户账户与密码,而用户也可以在此时通过“记住我的密码”选项,指定以后都通过这个用户账户连接该计算机。

3. 利用“映射网络驱动器”

右击“我的电脑”,选中“映射网络驱动器”,会出现如图 2-14 所示的对话框。在该对话框中,各部分的含义如下。

(1) 驱动器。此处请选择要用来连接共享文件夹的驱动器号,可以使用任何一个尚未被使用的驱动器号。

(2) 文件夹。请直接输入共享文件夹的通用命名约定(Universal Naming Convention,



图 2-14 "映射网络驱动器"对话框

UNC)路径，也就是"\\计算机名称\共享名"或者"\\IP 地址\共享名"，例如\\192.168.10.8\test，其中 192.168.10.8 为计算机 IP 地址，而 test 为共享名(不是文件夹的名称)。或者还可以单击"浏览"按钮完成连接的操作。

(3) 登录时重新连接。表示以后每次登录时，系统都会自动利用指定的驱动器号来连接该共享文件夹。

单击图 2-14 中的"完成"按钮后，就可以通过驱动器号访问共享文件夹内的文件，同时在"Windows 资源管理器"中会多一个"Z：驱动器"。

图 2-14 对话框中的其余两个选项如下。

① 使用其他用户名进行连接。系统默认是利用登录时所输入的用户账号与密码来连接共享文件夹，若该账户没有权限连接时，则可以在此处利用其他有权限的用户账户与密码连接。

② 注册联机存储或连接到网络服务器。可以通过此处在"网上邻居"内创建一个快捷方式，并且该快捷方式连接到此共享文件夹，该快捷方式还可以连接到网站内的文件夹或者 FTP 服务器内的文件夹。

4. 利用"运行"命令

用户还可以通过执行"开始"→"运行"命令，然后在"运行"对话框内输入 UNC 路径即可，例如\\192.168.10.8\test，单击"确定"按钮后窗口中就会显示该共享文件夹内的文件。

2.3.3 共享权限和 NTFS 权限的共同作用

1. 共享权限

用户必须拥有适当的共享权限，才能访问网络上共享文件夹的内容。表 2-1 列出共享权限的类型与允许的操作。默认情况下，允许 Everyone 组"读取"共享权限。

表 2-1　共享权限的类型与允许的操作

共享权限的类型与允许的操作	读取	修改	完全控制
查看该共享文件夹内的文件名称、子文件夹名称	√	√	√
查看文件内的数据、运行程序	√	√	√
遍历子文件夹	√	√	√
向该共享文件夹内添加文件、子文件夹		√	√
修改文件内的数据		√	√
删除文件与子文件夹		√	√
修改权限(只适用于 NTFS 内的文件和文件夹)			√
取得所有权(只适用于 NTFS 内的文件和文件夹)			√

注意：共享文件夹权限仅对通过网络访问该共享文件夹的用户有效。

与 NTFS 类似，共享文件夹中的权限也具有累加性，并且拒绝权限高于其他权限。如果将共享文件夹复制到其他的磁盘分区中，则原始的文件夹仍然保留共享的状态。但是复制的那个新的文件夹并不会被设为共享文件夹。如果将共享文件夹移动到其他的磁盘分区中，则该文件夹将不再是共享文件夹。

2. 与 NTFS 权限配合使用

在共享文件夹上设置了共享权限和 NTFS 权限后，网络上的用户在访问这个共享文件夹时，就要同时受到这两类权限的约束，即网络上的用户到底有没有权限访问该共享文件夹的内容，必须由共享权限与 NTFS 权限共同决定，并且有效权限是最严格的权限(也就是两种权限的交集)。

当用户从本地计算机直接访问文件夹的时候，不受共享权限的约束，只受 NTFS 权限的约束。

如果希望网络上的用户能够完全控制共享文件夹，首先要在共享权限中添加此用户(组)，并设置完全控制的权限。然后在 NTFS 权限设置中添加此用户(组)，也设置完全控制权限。只有两个地方都设置了完全控制权限，才最终有完全控制权限。

例如，如果用户 A 对共享文件夹 C:\Test 的有效共享权限为“读取”，并且用户对该文件的有效 NTFS 权限为“完全控制”，则用户 A 对 C:\Test 的最终有效权限为两者之中最为严格的“读取”。如果用户 A 直接从本地登录，而不是通过网络登录，则用户 A 对 C:\Test 的有效权限由 NTFS 权限决定，也就是“完全控制”。

如果两个权限存在冲突，例如，共享权限为只读，NTFS 权限是写入，那么最终权限是完全拒绝，因为最终的权限是这两个权限的交集。

第3章　磁盘管理

学习目标

学习完本章后，应该了解 Windows Server 2003 磁盘类型；了解基本磁盘与动态磁盘的区别及其特点；能够运用 Windows Server 2003 磁盘管理工具来管理磁盘，掌握磁盘分区的创建与管理、卷的创建与管理以及如何将基本磁盘升级到动态磁盘；掌握常见的磁盘管理任务的一些基本操作方法。

3.1　磁盘类型

在 Windows Server 2003 中，将磁盘分为基本磁盘和动态磁盘两种类型。默认情况下，磁盘最初被配置为基本磁盘。

3.1.1　基本磁盘

在基本磁盘能够存储数据之前，该磁盘必须被划分成一个或多个磁盘分区。磁盘分区就是把一个基本物理磁盘分成若干部分，称为分区的每部分都能作为一个独立单元工作。

基本磁盘最多可以创建 4 个主磁盘分区，或最多 3 个主磁盘分区加上一个扩展分区。扩展分区必须划分为一个或多个逻辑驱动器以后才能使用。在一个基本磁盘上可以创建多达 24 个逻辑驱动器。

3.1.2　动态磁盘

1. 动态磁盘的类型

动态磁盘支持多种类型的动态卷，分别如下。

1）简单卷

简单卷只能包含单个物理磁盘，即磁盘空间来自同一个物理磁盘。只能在动态磁盘上创建简单卷。简单卷支持 NTFS、FAT 或 FAT32 文件系统。简单卷比基本磁盘的分区限制更少，例如简单卷没有空间大小限制，也没有对在单个磁盘上可创建卷的数量的限制。如果简单卷不是系统卷或启动卷，则可以在同一磁盘内对其进行扩展，也可扩展到其他磁盘上。如果跨多个磁盘扩展简单卷，则该卷将成为跨区卷。要扩展简单卷，该卷必须使用 NTFS 文件系统格式化或未被格式化。简单卷不支持容错，但可以被镜像。

2）跨区卷

跨区卷由两个或多个动态磁盘上的可用空间组成，来自不同磁盘的空间不必相同，可以通过扩展增加跨区卷的容量，也可以将多个动态磁盘上的未指派空间合并成一个跨区卷，并分配一个逻辑驱动器号。只能在动态磁盘上创建跨区卷。写入数据时，在第一个磁盘写满后，数据才会写入跨区卷的下一个磁盘中。跨区卷可以提高读的性能，但不支持容错，也不能被镜像。

3）带区卷

带区卷（RAID 0）由两个或多个动态磁盘上的未指派的空间组成，来自不同磁盘的空间必须相同。只能在动态磁盘上创建带区卷。数据写入时以 64KB 为单位被平均、交替地写到每个磁盘内，带区卷读写性能最好，但不提供容错。如果带区卷中的磁盘发生故障，则整个卷中的数据都将丢失。带区卷不能被镜像或扩展。

4）镜像卷

镜像卷（RAID 1）由一个动态磁盘内的简单卷与另一个动态磁盘内的未指派空间组成，或是由将两个动态磁盘上的未指派的空间组成，这两个空间必须相同，并分配一个逻辑驱动器号。数据同时向两块磁盘写，提高读的性能，这两个磁盘区域内将存储完全相同的数据。如果镜像卷中的一个动态磁盘出现故障，还有另一个磁盘上可以继续读写数据，镜像卷磁盘利用率为 50%，提供容错，镜像卷不能被扩展。

5）RAID-5 卷

RAID-5 卷由 3 个或更多个动态磁盘的未指派空间组成，来自不同磁盘的空间必须相同，然后分配一个逻辑驱动器号。数据同时向多块磁盘操作，提高读、写性能。RAID-5 卷是一种带有数据和奇偶校验带区的容错卷。奇偶校验是用于在发生故障后重建数据的计算值。如果物理磁盘的某一部分发生故障，Windows 会从其余的数据和奇偶校验重新创建发生故障的那部分磁盘上的数据，让系统能够继续工作。RAID-5 卷提供单点失败容错，磁盘利用率为 $(n-1)/n\times100\%$，RAID-5 卷无法被镜像或扩展。

2. 动态磁盘的优点

与基本磁盘相比，动态磁盘的优点如下。

（1）基本磁盘可以最多创建 4 个主磁盘分区，或最多 3 个主磁盘分区加上一个扩展分区。而动态磁盘没有卷数量的限制，只要有足够的磁盘空间。

（2）在基本磁盘中，分区是不可跨越磁盘的。而动态磁盘可以将多块磁盘中的空余磁盘空间扩展到同一个卷中。

（3）基本磁盘的读写速度由硬件决定。而利用动态磁盘，可以创建带区卷提升磁盘的读写效率。

（4）基本磁盘没有容错性。而利用动态磁盘，可以创建镜像卷或 RAID-5 卷，保证在提高读写性能的同时，也提供容错。

3.2 磁盘管理控制台

打开“磁盘管理”的操作步骤为：打开“计算机管理”管理工具，展开“存储”→“磁盘管理”即可，如图 3-1 所示。

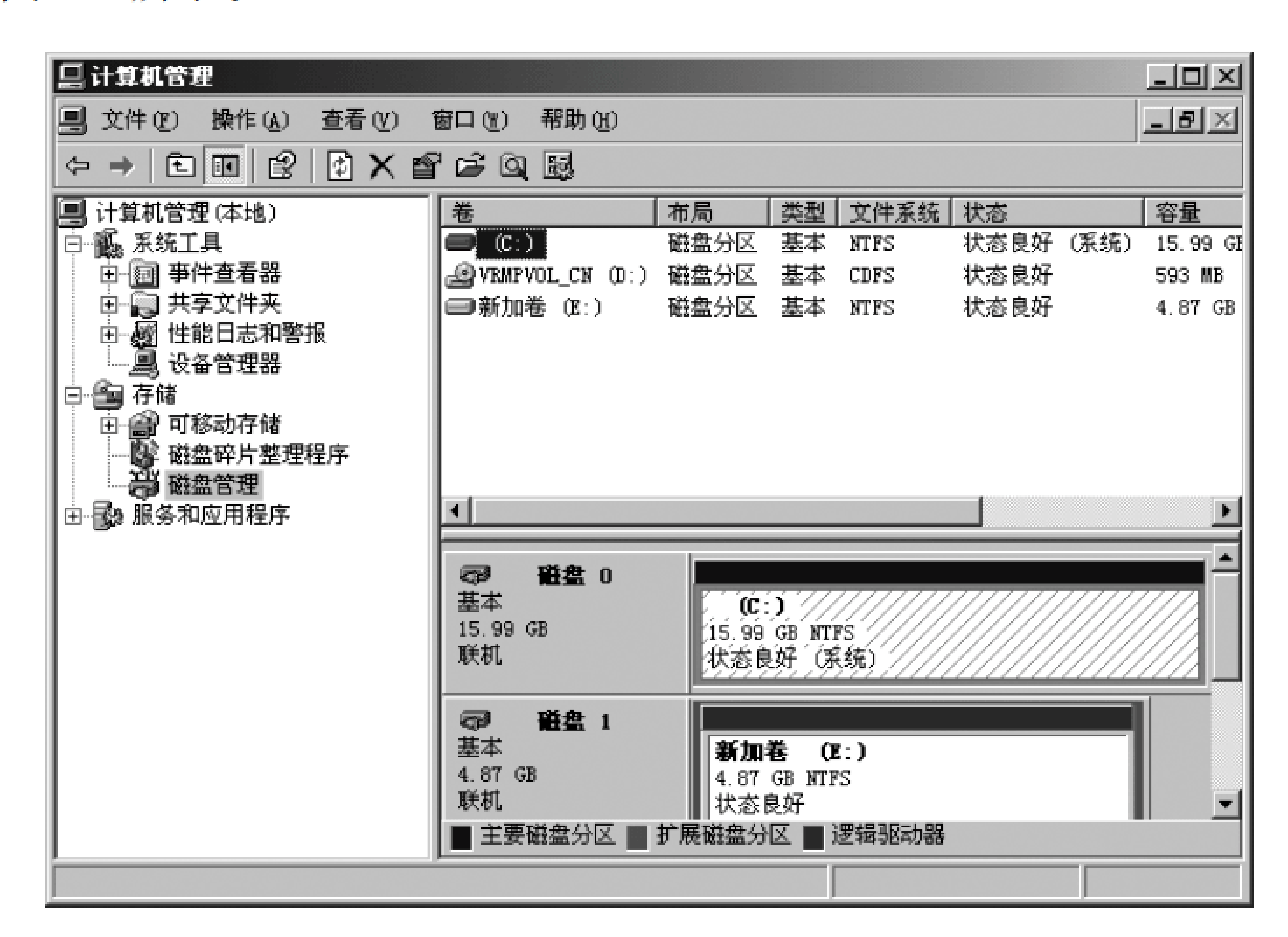


图 3-1 打开“计算机管理”窗口

利用磁盘管理控制台，可以查看文件系统类型、运行状态、容量等，也可以进行格式化分区、更改驱动器名、将基本磁盘转换为动态磁盘等操作。

3.3 分区的创建与管理

1. 创建磁盘分区

假设要创建一个主磁盘分区，操作步骤如下。

(1) 在“计算机管理”对话框中，选择“磁盘管理”。

(2) 右击没有创建磁盘分区的磁盘，在弹出的快捷菜单中选择“新建磁盘分区”，弹出“欢迎使用新建磁盘分区向导”。

(3) 在“欢迎使用新建磁盘分区向导”中选择“主磁盘分区”，单击“下一步”按钮。

(4) 设置主磁盘分区的大小，并指派驱动器号。

(5) 接下来选择是否要对其进行格式化。如果需要格式化，要求设定文件系统类型、分配单位大小并设置卷标。

2. 格式化磁盘分区

要格式化磁盘分区，操作步骤如下。

(1) 在“计算机管理”对话框的右边选择要格式化的磁盘分区，右击该磁盘分区，选择

“格式化”菜单项，如图 3-2 所示。



图 3-2 “计算机管理”窗口

(2) 单击“格式化”选项，弹出“格式化”对话框，根据要求输入卷标、选择文件系统和分配单位大小，并根据实际需要选择“执行快速格式化”和“启用文件和文件夹压缩”复选框。如图 3-3 所示，单击“确定”按钮。

(3) 单击“确定”按钮，弹出“警告信息”，如图 3-4 所示。单击“确定”按钮完成格式化操作，单击“取消”按钮便可取消该磁盘分区的格式化操作。



图 3-3 “格式化”对话框

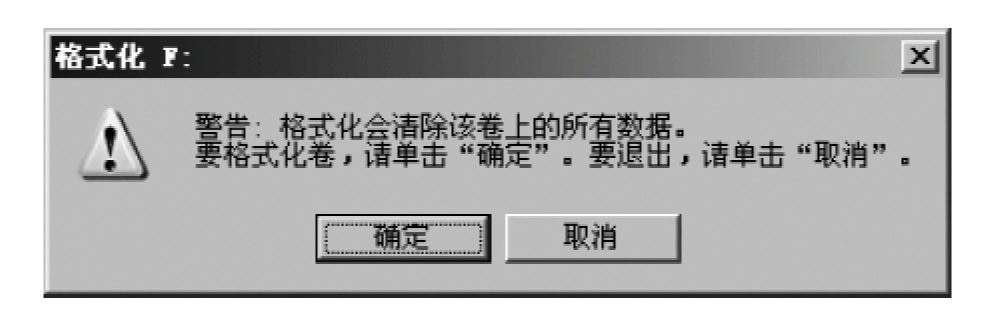


图 3-4 “格式化”警告信息

3.4 卷的创建与管理

3.4.1 从基本磁盘转换为动态磁盘

1. 转换前的注意事项

将基本磁盘转换到动态磁盘之前，需要注意的事项如下。

(1) 要执行转换，用户必须是本地计算机 Backup Operators 组或 Administrators 组

的成员，或者必须被委派了适当的权限。

（2）将基本磁盘转换为动态磁盘后，如果又想使用基本磁盘的分区，则必须先将数据备份到另一个卷上，删除动态磁盘上的所有动态卷后，再使用“转换成基本磁盘”命令。

（3）在转换磁盘之前，请关闭这些磁盘上运行的所有程序。

（4）将基本磁盘转换为动态磁盘后，基本磁盘上全部现有分区都将变为动态磁盘上的简单卷。

（5）不要将包含 Windows 2000、Windows XP Professional 或 Windows Server 2003 多操作系统的磁盘转换为动态磁盘。因为这样只能启动当前启动的系统，无法再启动第二个系统。

（6）便携式计算机、可移动磁盘、使用通用串行总线（USB）或 IEEE 1394（也称为“火线”）接口的可分离磁盘，以及连接到共享小型计算机系统接口（Small Computer System Interface，SCSI）总线的磁盘并不支持动态磁盘。

（7）不能将已连接到共享 SCSI 或光纤通道总线的群集磁盘转化为动态磁盘（群集服务只支持基本磁盘）。

2. 将基本磁盘转换为动态磁盘

要将基本磁盘转换为动态磁盘，操作步骤如下。

（1）右击“我的电脑”，在弹出的快捷菜单中选择“管理”后，会出现“计算机管理”对话框。

（2）右击需要转换的磁盘，在弹出的快捷菜单中选择“转换到动态磁盘”，如图 3-5 所示。



图 3-5 “转换到动态磁盘”菜单

（3）出现如图 3-6 所示的“转换为动态磁盘”对话框后，选中需要转换的磁盘，单击“确定”按钮，出现如图 3-7 所示的对话框后，选中要转换的磁盘，再单击“转换”按钮，即可

开始转换。

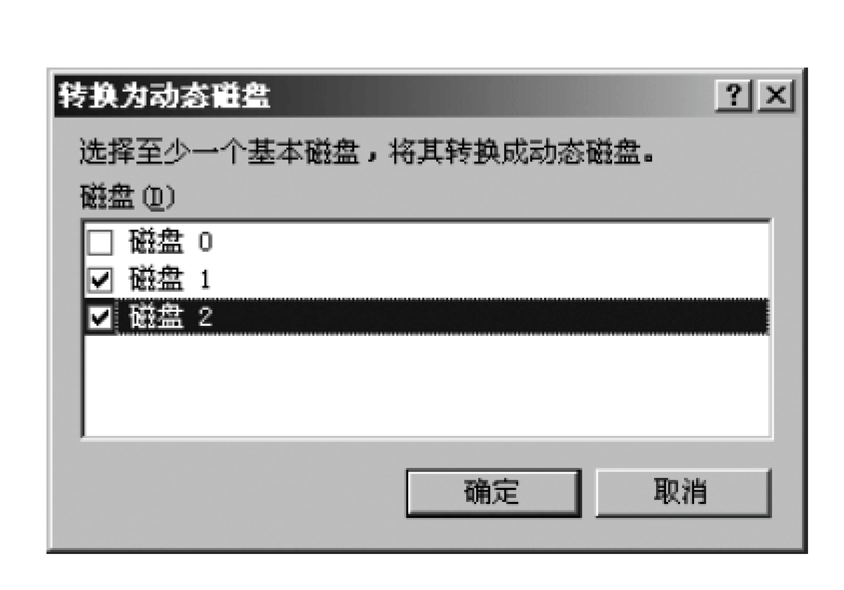


图 3-6 “转换为动态磁盘”对话框

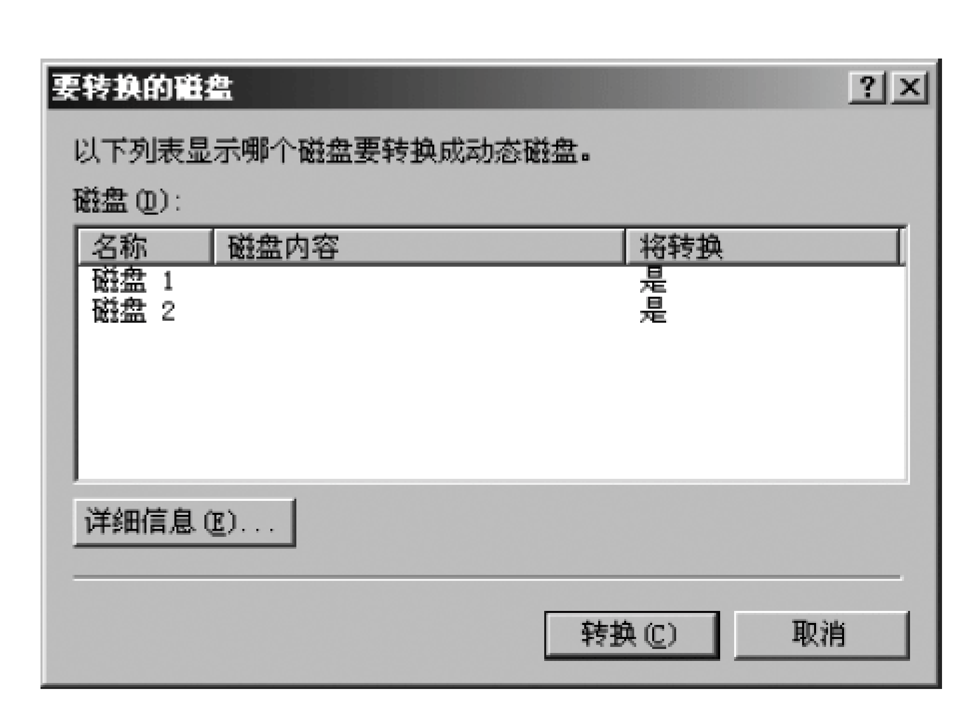


图 3-7 “要转换的磁盘”对话框

(4) 接下来按照系统提示继续操作，转换完成后需要重新启动计算机，以便完成转换工作。

3.4.2 创建、扩展简单卷

简单卷是动态磁盘中的基本单位，与基本磁盘中的主磁盘分区相当。可以使用一个动态磁盘内的未指派空间来创建简单卷，并可以扩展简单卷。

1. 创建简单卷

创建简单卷的操作步骤为如下。

(1) 右击一块未指派的空间，在弹出的快捷菜单中选择“新建卷”。

(2) 出现“新建卷向导”对话框后，选择要创建的卷的类型为“简单”，然后单击“下一步”按钮，如图 3-8 所示。

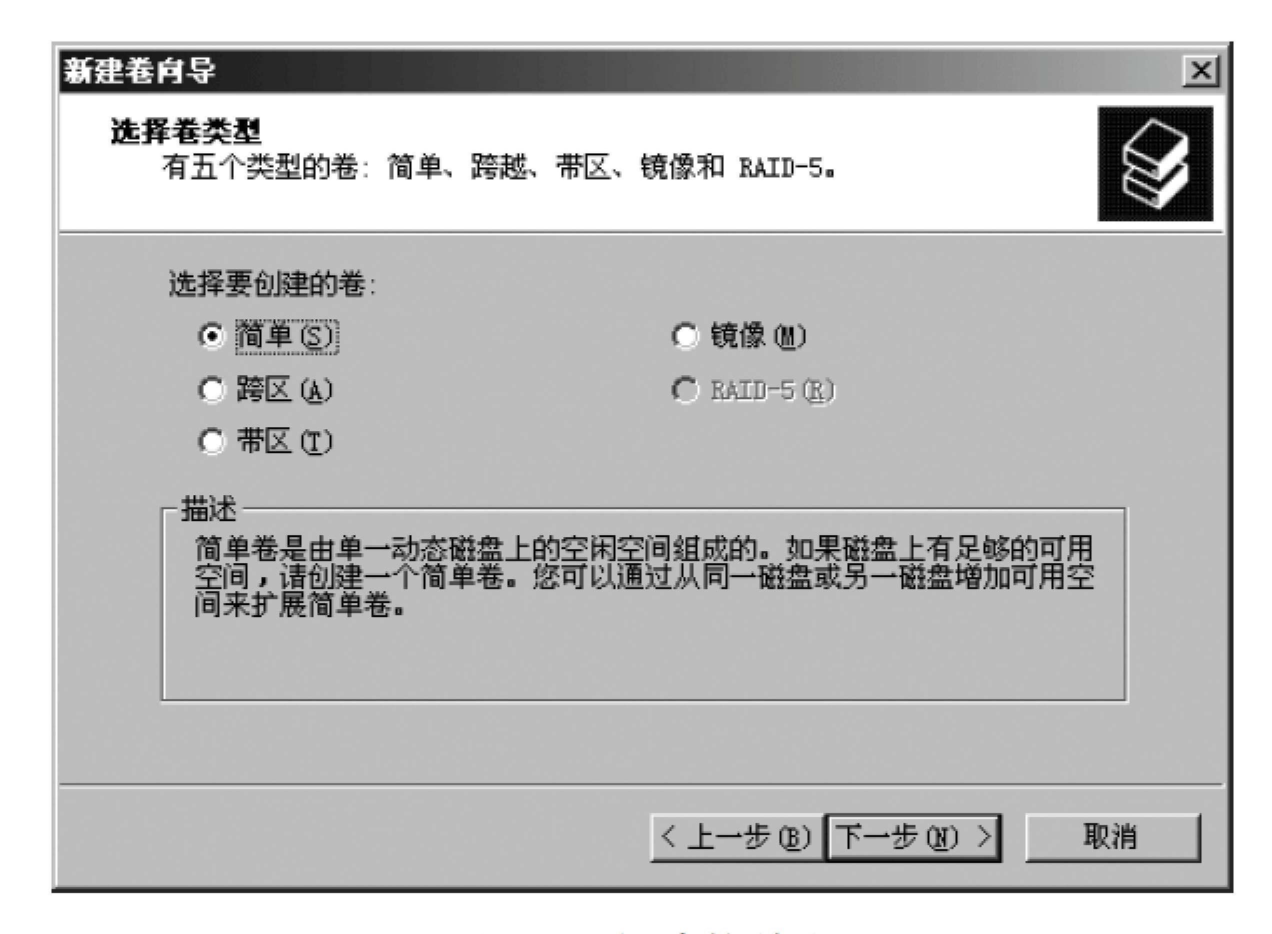


图 3-8 新建简单卷

(3) 出现如图 3-9 所示的对话框时,需要设置该简单卷的大小,然后单击“下一步”按钮。

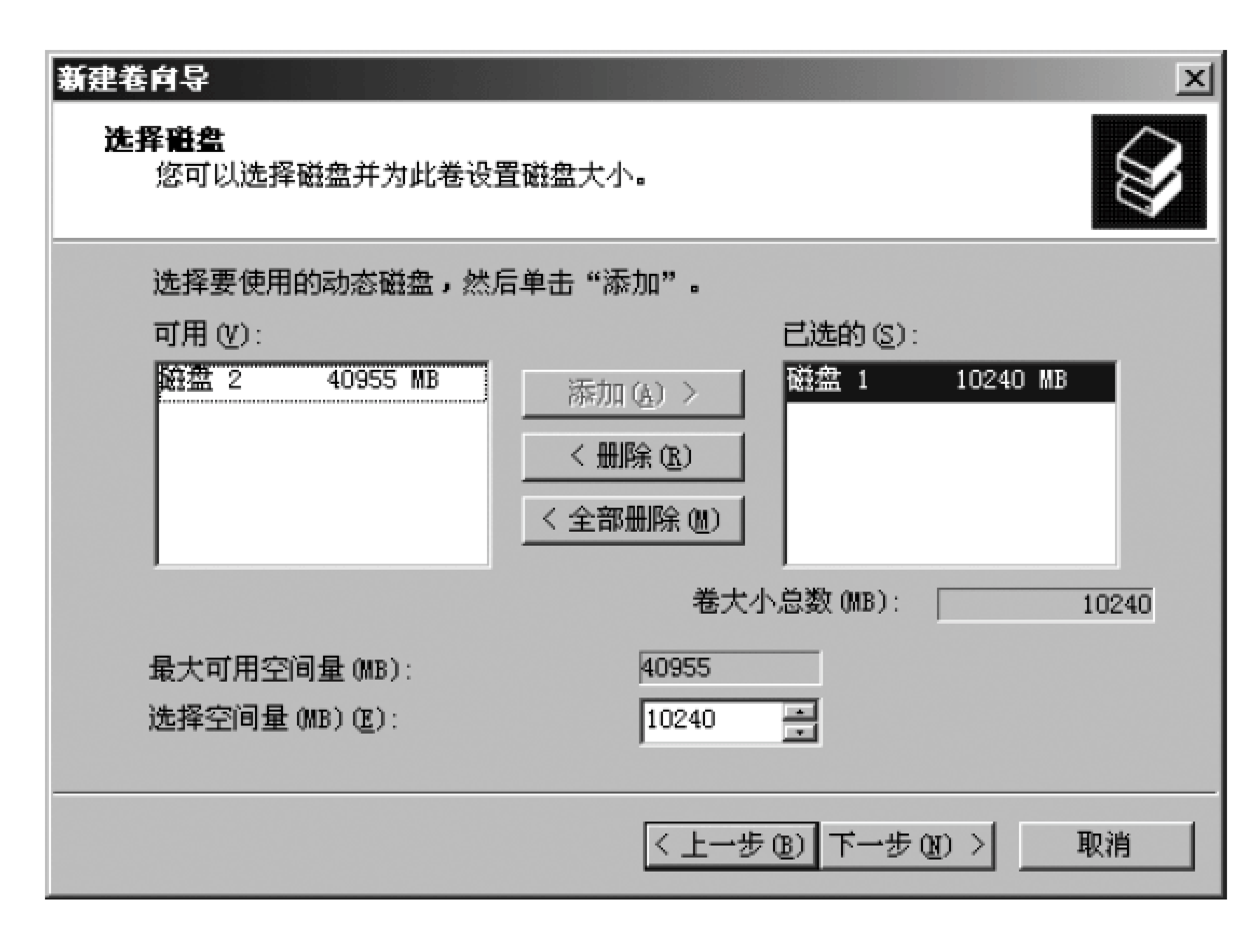


图 3-9 设置简单卷大小

(4) 出现如图 3-10 所示的对话框时,指派一个驱动器号代表该简单卷,然后单击“下一步”按钮。

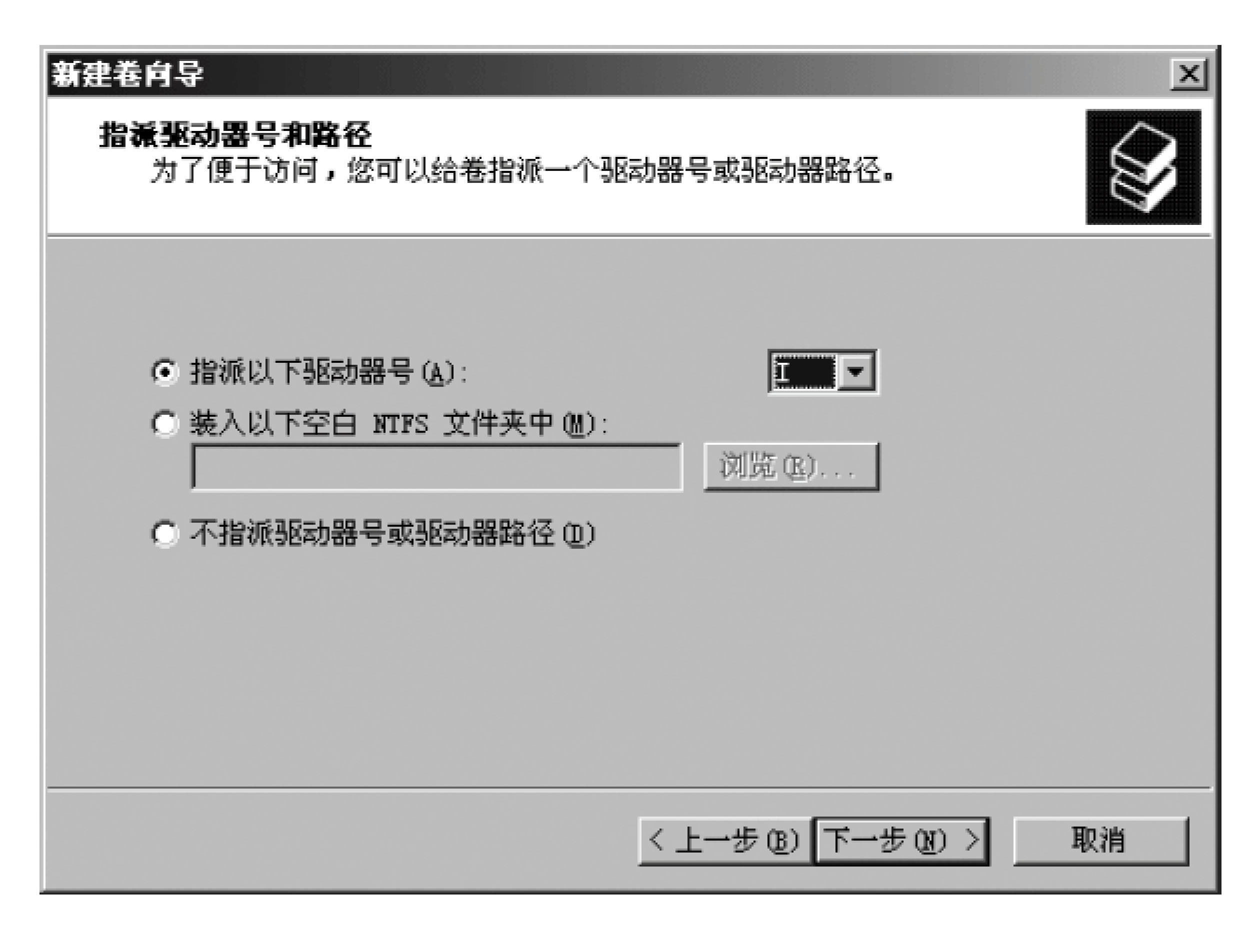


图 3-10 指派简单卷的驱动器号

(5) 在图 3-11 所示的对话框中进行设置,其中各项的含义分别如下。

① 文件系统。可以选择将其格式化为 FAT、FAT32 或 NTFS 的文件系统。

② 分配单位大小。分配单位是磁盘的最小访问单位。分配单位的大小必须适当,过大或过小都不好。除非有特殊的需求,否则此处建议选用默认值,系统会根据此分区的大小自动设置最适当的分配单位大小。

③ 卷标。为此磁盘分区设置一个名称。

④ 执行快速格式化。它只会重新创建 FAT、FAT32 或 NTFS 格式,但不会检查是否有坏扇区。在选择该选项之前,需要先确定磁盘内没有坏扇区,才能选择快速格式化。

⑤ 启用文件和文件压缩。将该磁盘分区设为“压缩磁盘”，以后添加到该磁盘分区中的文件和文件夹都会被自动压缩。

设置完成后，在图 3-11 中单击“下一步”按钮。

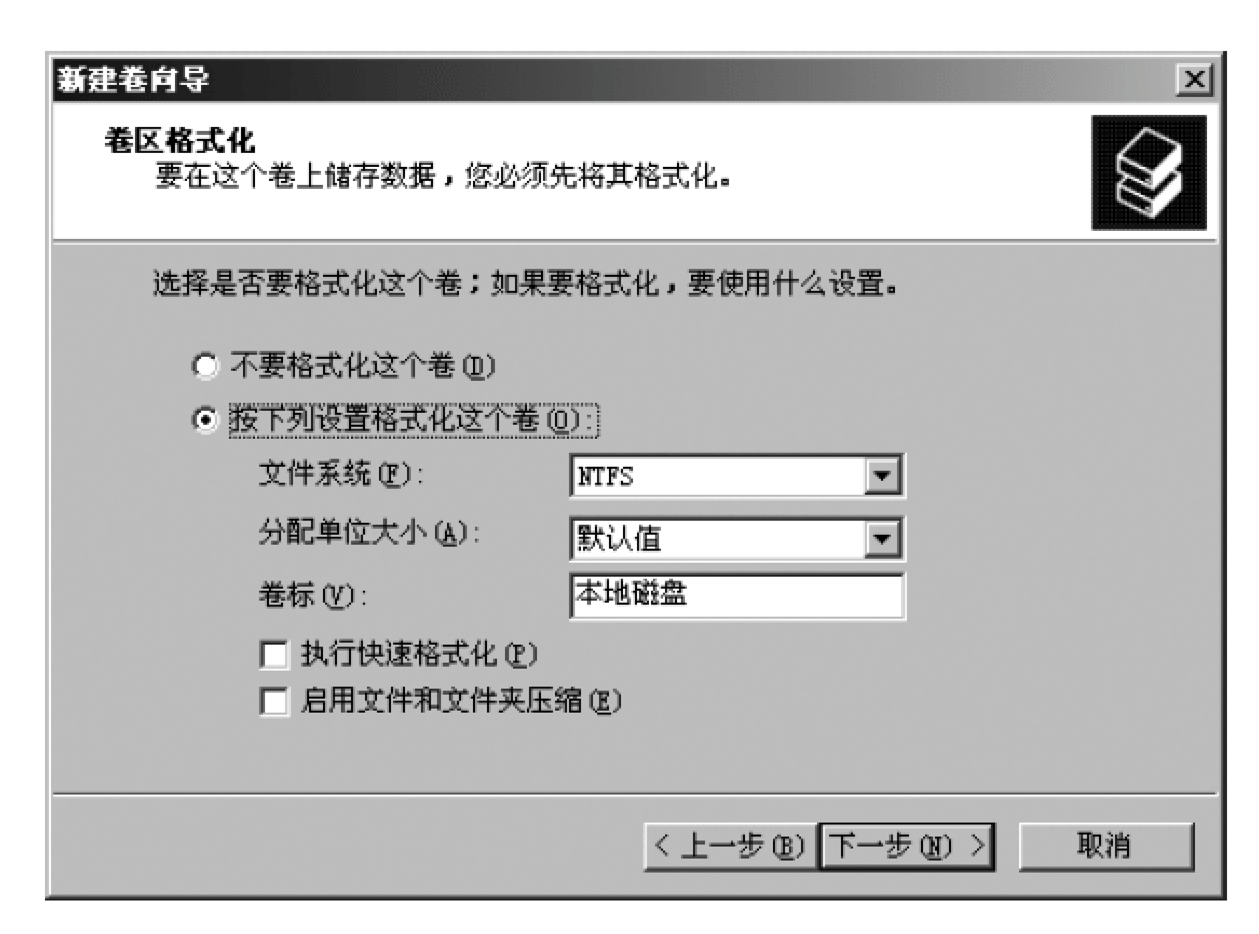


图 3-11　设置简单卷的格式化

(6) 出现“正在完成新建卷向导”对话框后，单击“完成”按钮，系统就会完成该卷的创建，如图 3-12 所示。

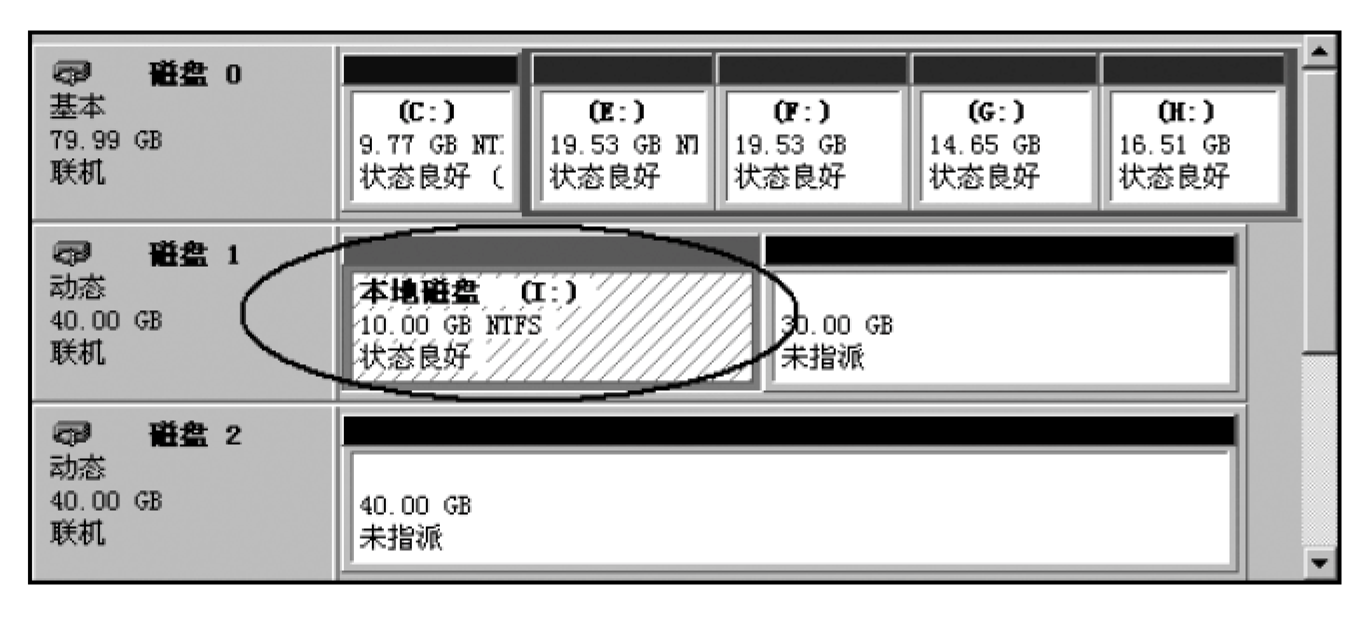


图 3-12　完成新建简单卷

2. 简单卷的扩展

要扩展简单卷，需要注意的是：

(1) 仅能扩展未格式化或使用 NTFS 文件系统格式化的卷，不能扩展用 FAT 或 FAT32 格式化的卷。

(2) 不能扩展系统卷、启动卷、带区卷、镜像卷或 RAID-5 卷。

(3) 只要具有可用磁盘空间，就可以扩展不是系统或启动卷的简单卷或扩展卷。

(4) 如果将 Windows 2000 升级到 Windows XP Professional 或 Windows Server 2003，则无法扩展最初在 Windows 2000 上作为基本卷创建的、然后转换为动态卷的简单卷或跨区卷。

扩展卷的操作步骤如下。

(1) 在“计算机管理”对话框中,选中“磁盘管理”。

(2) 右击要扩展的简单卷或跨区卷,然后单击“扩展卷”,并按屏幕上的指示操作即可,可参照上述“创建卷”时的操作步骤。

3.4.3 创建跨区卷、带区卷、镜像卷和 RAID-5 卷

跨区卷、带区卷、镜像卷和 RAID-5 卷的创建与基本卷的创建过程类似,只是在图 3-8 所示的对话框中选择不同卷的类型即可。

(1) 在创建跨区卷之前,需要注意的是:

① 跨区卷的每个成员的容量大小可以不同。

② 跨区卷的成员中不可以包含“系统卷”与“引导卷”。

③ 整个跨区卷是一体的,无法独立使用其中任何一个成员,除非将整个跨区卷删除。

(2) 在创建带区卷之前,需要注意的是:

① 带区卷的每个成员的容量大小必须相同。

② 带区卷的成员不可以包含系统卷与引导卷。

③ 带区卷一旦被创建好后,就无法再扩展,除非将其删除后再重建。

④ 整个带区卷是一体的,无法独立使用其中任何一个成员,除非将整个带区卷删除。

(3) 在创建镜像卷之前,需要注意的是:

① 镜像卷的成员只有 2 个,并且它们必须是位于不同的动态磁盘内。用户可以选择一个简单卷与一个未指派的空间,或者两个未指派的空间组合成镜像卷。

② 如果选择将一个简单卷与一个未指派空间组成镜像卷,则系统在创建镜像卷的过程中,会将简单卷内的现有数据复制到另一个成员中。

③ 组成镜像卷的 2 个卷的容量大小必须相同。

④ 组成镜像卷的成员中,可以包含系统卷与引导卷。

⑤ 镜像卷一旦被创建好后,就无法再被扩展。

⑥ 只有 Windows Server 2003、Windows Server 2000 系列产品才支持镜像卷。

⑦ 整个镜像卷是一体的,如果要独立使用其中任何一个成员,则必须先中断镜像关系、删除镜像或删除该镜像卷。

⑧ 由于两个磁盘内存储重复的数据,因此镜像卷的磁盘空间使用率只有 50%。

(4) 在创建 RAID-5 卷之前,需要注意的是:

① RAID-5 卷的每个成员的容量大小必须相同。

② RAID-5 卷的成员不可以包含“系统卷”和“启动卷”。

③ RAID-5 卷的磁盘空间有效使用率为$(n-1)/n$,n 为磁盘的数目。例如,如果利用 5 个磁盘来创建 RAID-5 卷,则必须利用 1/5 的磁盘空间来存储奇偶校验数据,因此磁盘空间的有效使用率为 4/5。

④ RAID-5 卷一旦被创建好后,就无法再被扩展。

⑤ 整个 RAID-5 卷是一体的,无法独立使用其中任何一个成员,除非将整个 RAID-5 卷删除。

3.5 常见的磁盘管理任务

3.5.1 查看磁盘的状态和属性

要在本地计算机上查看磁盘的状态和属性，用户必须是本地计算机 Backup Operators 组或 Administrators 组的成员，或者被委派了适当的权限。要查看磁盘的状态和属性，操作步骤如下。

(1) 打开“计算机管理(本地)”。

(2) 在控制台树中，选择“计算机管理(本地)”→“存储”→“磁盘管理”。

(3) 在图形视图或磁盘列表中，右击磁盘，选择“属性”。

3.5.2 修复、删除分区和卷

1. 修复分区和卷

镜像卷与 RAID-5 卷都具备容错的功能，如果成员中有一个磁盘出现故障，系统还能够正常工作，但丧失容错的功能，此时应该尽快地修复故障磁盘，以便继续提供容错的功能。

1) 镜像卷的修复

假设磁盘 1 和磁盘 2 中存在镜像卷，如果磁盘 2 中的镜像卷出现故障，此时，应该删除磁盘 2 上对应的磁盘 1 上的镜像卷，然后重新为磁盘 1 的镜像卷“添加镜像”。在此，以图 3-13 磁盘阵列(已建立简单卷、跨区卷、带区卷、镜像卷和 RAID-5 卷)为例来操作镜像卷的修复。

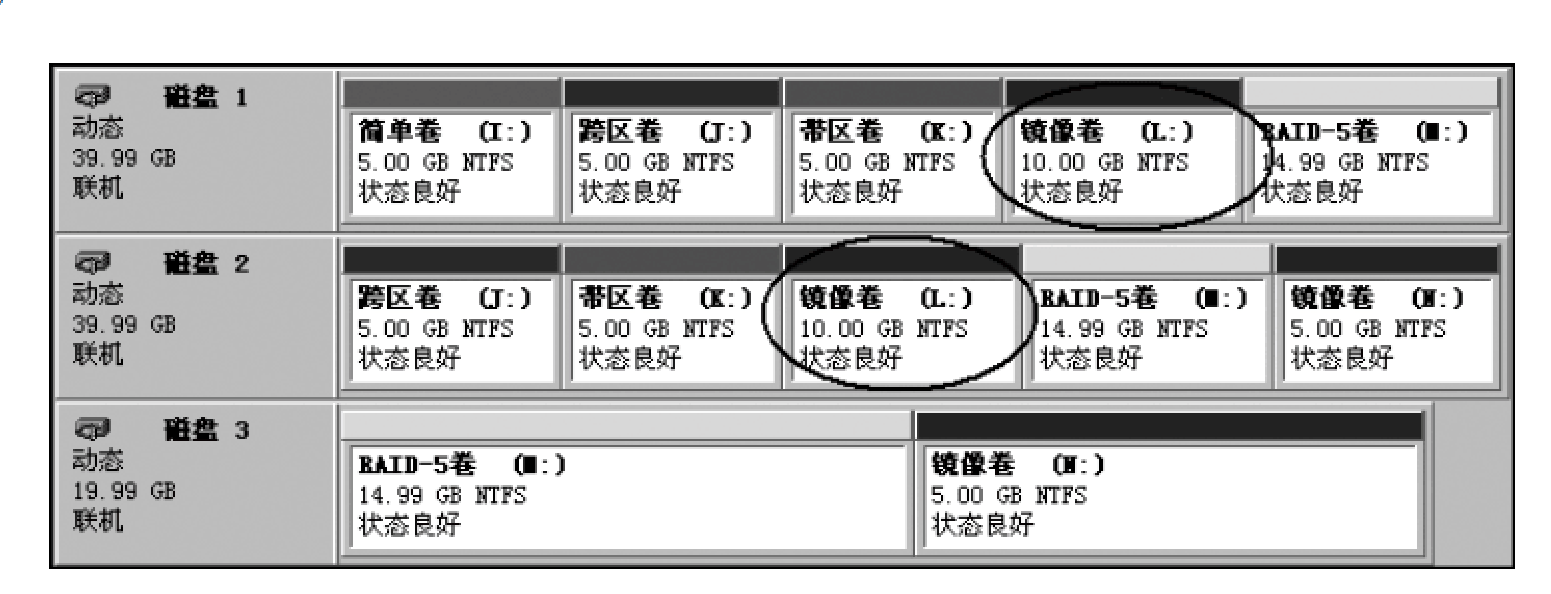


图 3-13 磁盘阵列

在图 3-13 中可以看出，磁盘 1 的镜像卷“L：”的镜像为磁盘 2 的镜像卷“L：”，假设磁盘 2 上的镜像卷“L：”已出现故障，在该卷上右击，在弹出的快捷菜单中单击“删除镜像”按钮，弹出如图 3-14“删除镜像”对话框。

在图 3-14“删除镜像”对话框中，选中要删除的镜像卷所在的磁盘，然后单击“删除镜像”按钮，此时会弹出对话框询问是否确实要删除镜像卷，单击“是”按钮。删除该故障磁盘镜像卷后，结果如图 3-15 所示。

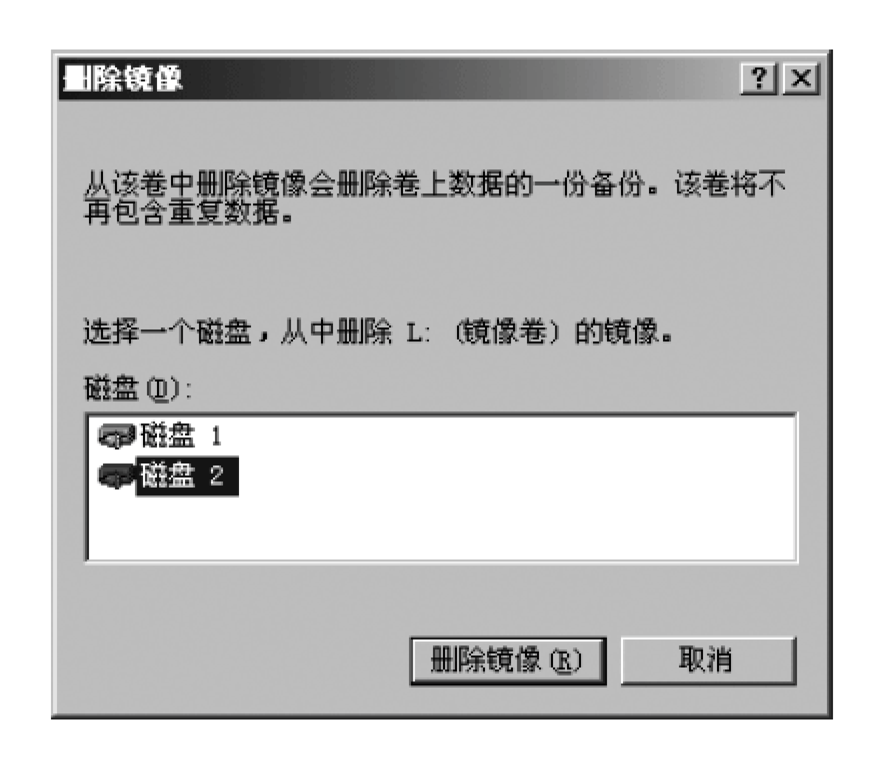


图 3-14 “删除镜像”对话框

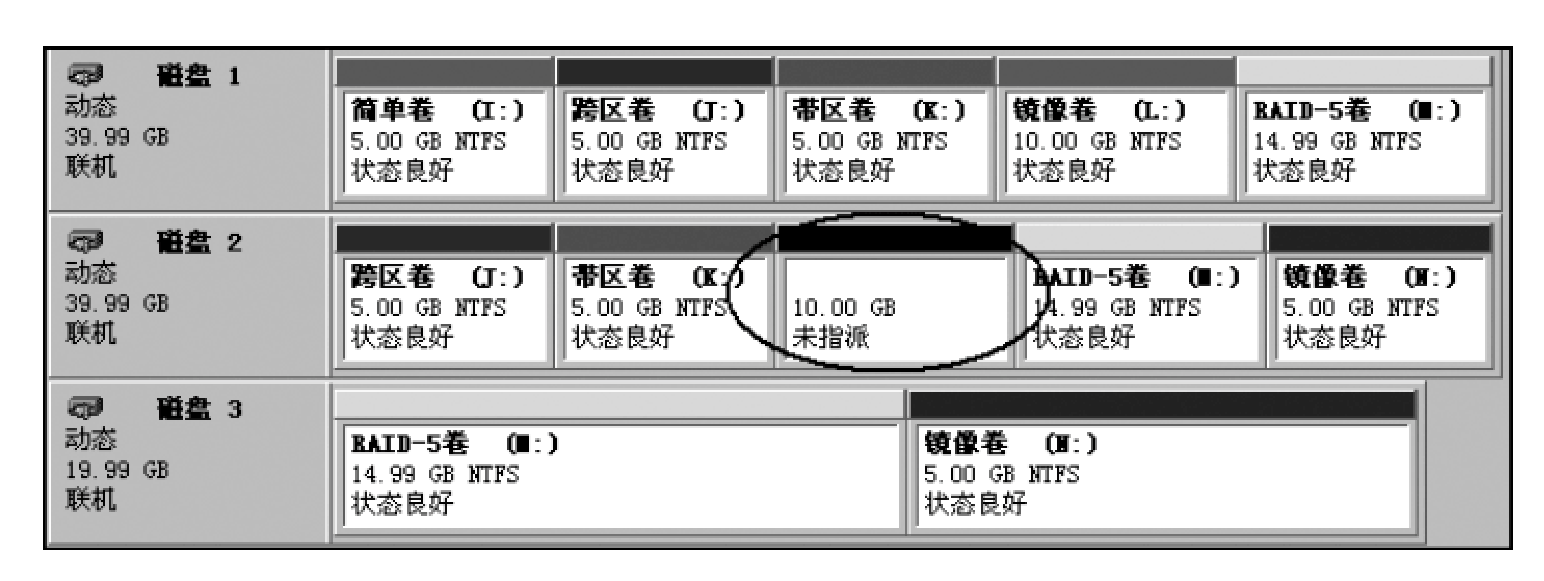


图 3-15 删除镜像后的结果

在图 3-15 中可以发现磁盘 1 上的镜像卷的颜色已发生变化了，这就说明磁盘 1 上的镜像卷“L：”已不存在镜像。为了保证磁盘 1 的镜像卷“L：”的修复功能，可以为该镜像卷“添加镜像”。

在磁盘 1 中的镜像卷上右击，在弹出的快捷菜单中单击“添加镜像”命令，弹出如图 3-16 所示的“添加镜像”对话框，选中磁盘 2，然后单击“添加镜像”按钮。

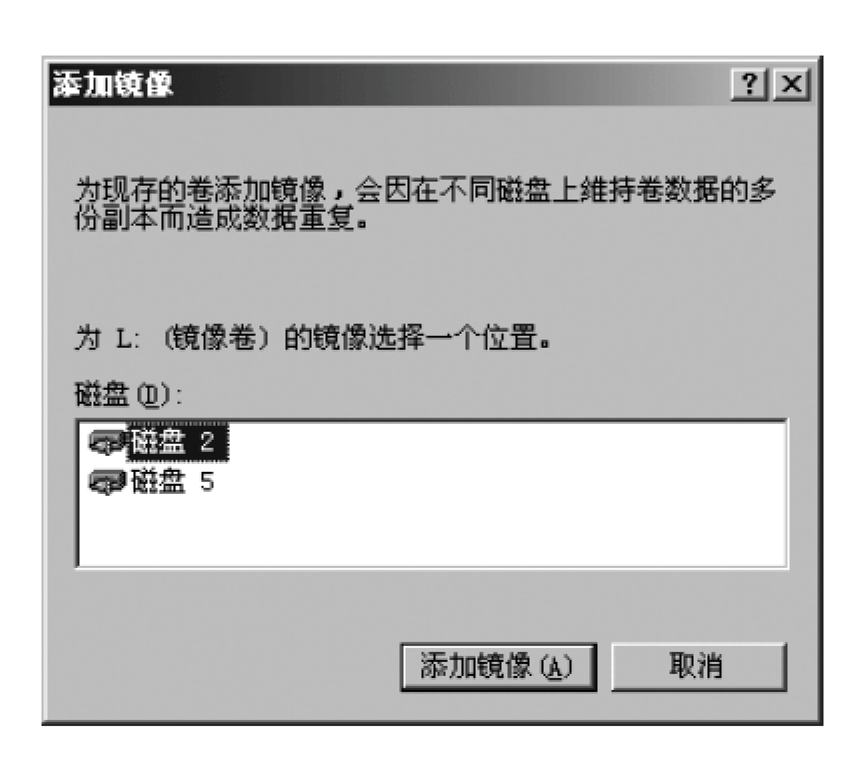


图 3-16 “添加镜像”对话框

磁盘 1 的镜像卷“L：”“添加镜像”成功后的结果如图 3-17 所示。此时，磁盘 1 的镜像卷“L：”会与磁盘 2 的镜像卷“L：”进行“重新同步”。待“重新同步”完成后，磁盘 1 的镜像卷“L：”的镜像卷添加也就完成了。

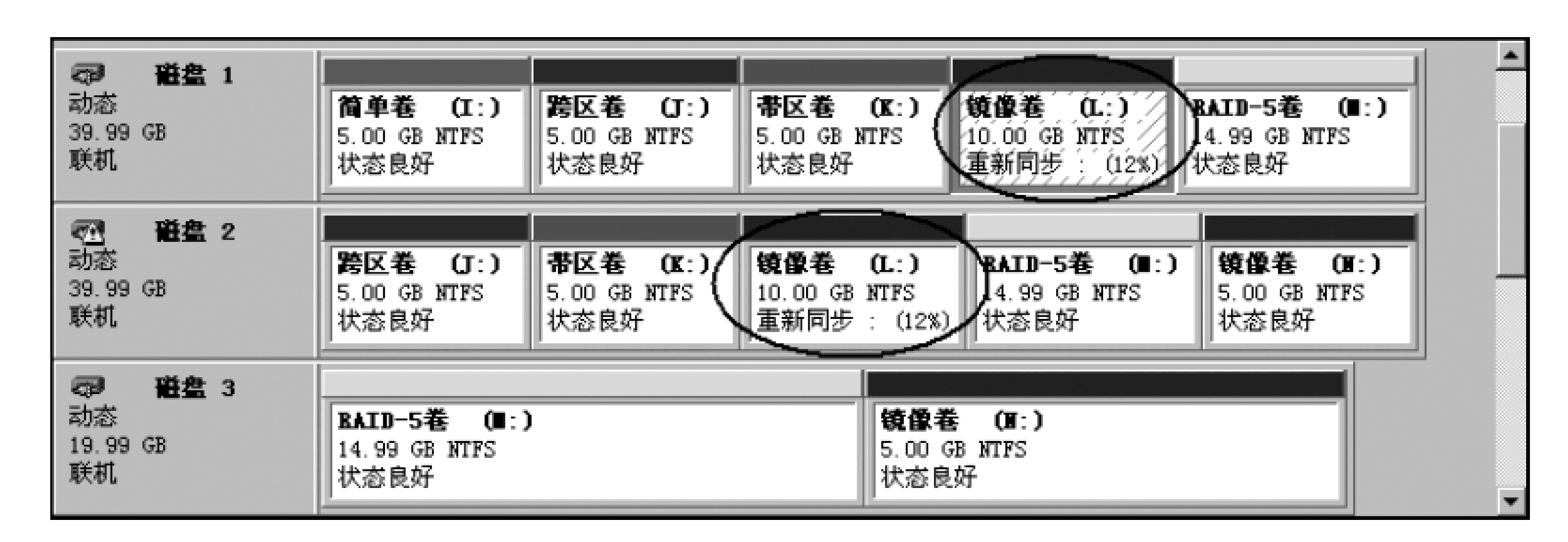


图 3-17 "添加镜像"后的结果

当磁盘 1 或磁盘 2 的镜像卷出现故障后，就可以使用其中一个没有故障的镜像卷来添加镜像，这也正体现了镜像卷的修复功能。

2) RAID-5 卷的修复

以图 3-18 磁盘阵列为例，说明如何修复 RAID-5 卷，以便恢复其容错功能。



图 3-18 磁盘阵列

假设其中成员中的磁盘 3 出现故障，则 RAID-5 的修复步骤如下。

(1) 将出现故障的磁盘 3 从计算机内拔出来。

(2) 将新的磁盘安装到计算机内。

(3) 启动计算机后，运行"计算机管理"。

(4) 如果出现"欢迎使用初始化和转换磁盘向导"对话框时，则单击"下一步"按钮，否则直接跳到第(7)步。

(5) 在如图 3-19 所示的对话框中，选择要初始化的磁盘，然后选择要转换为动态磁盘的磁盘。

(6) 出现"完成初始化和转换磁盘向导"对话框时，请单击"完成"按钮。

(7) 出现如图 3-20 所示的画面，其中的磁盘 3 为新安装的磁盘，而原先属于 RAID-5 卷的故障磁盘 3 被显示在画面的最下方(上面有"丢失"两个字)。接下来，在图 3-21 所示有"失败的重复"字样的任何一个"K："磁盘右击，在弹出的快捷菜单中选择"修复卷"。



图 3-19　磁盘初始化和转换向导

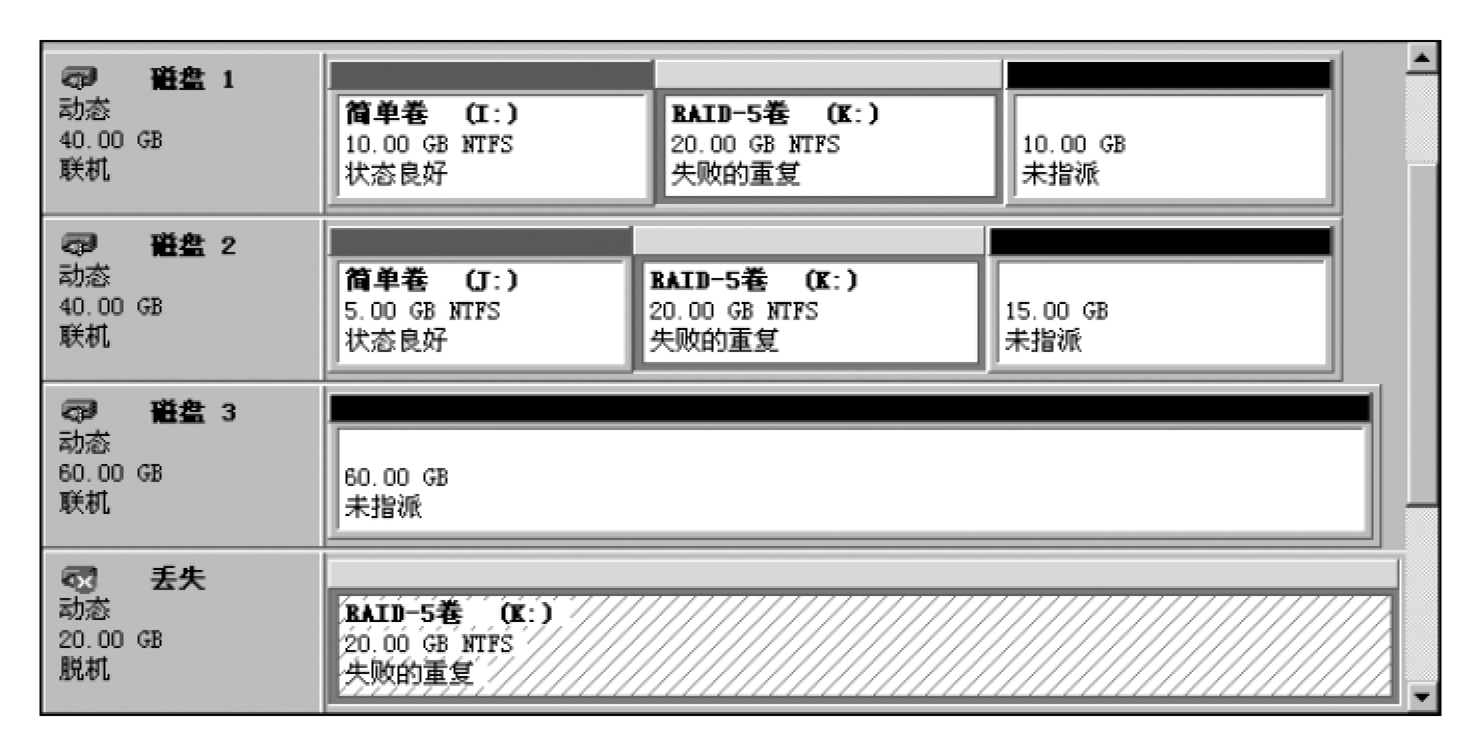


图 3-20　新加磁盘初始化和转化



图 3-21　RAID-5 卷“修复卷”命令

(8) 在如图 3-22 所示的对话框中，选择一块磁盘(例如磁盘 3)，它将被用来取代原先已损毁的磁盘，以便重新创建 RAID-5 卷。



图 3-22 “恢复 RAID-5 卷”对话框

(9) 系统会利用 RAID-5 卷中其他正常磁盘的内容，将数据重建到新磁盘内(同步)，等“重新同步”完成后，如图 3-23 所示，图中的“K：”又恢复了正常的 RAID-5 卷。



图 3-23 恢复 RAID-5 卷后的结果

(10) 如图 3-24 所示，右击标记为“丢失”的磁盘，在弹出的快捷菜单中选择“删除磁盘”命令将这个磁盘删除。

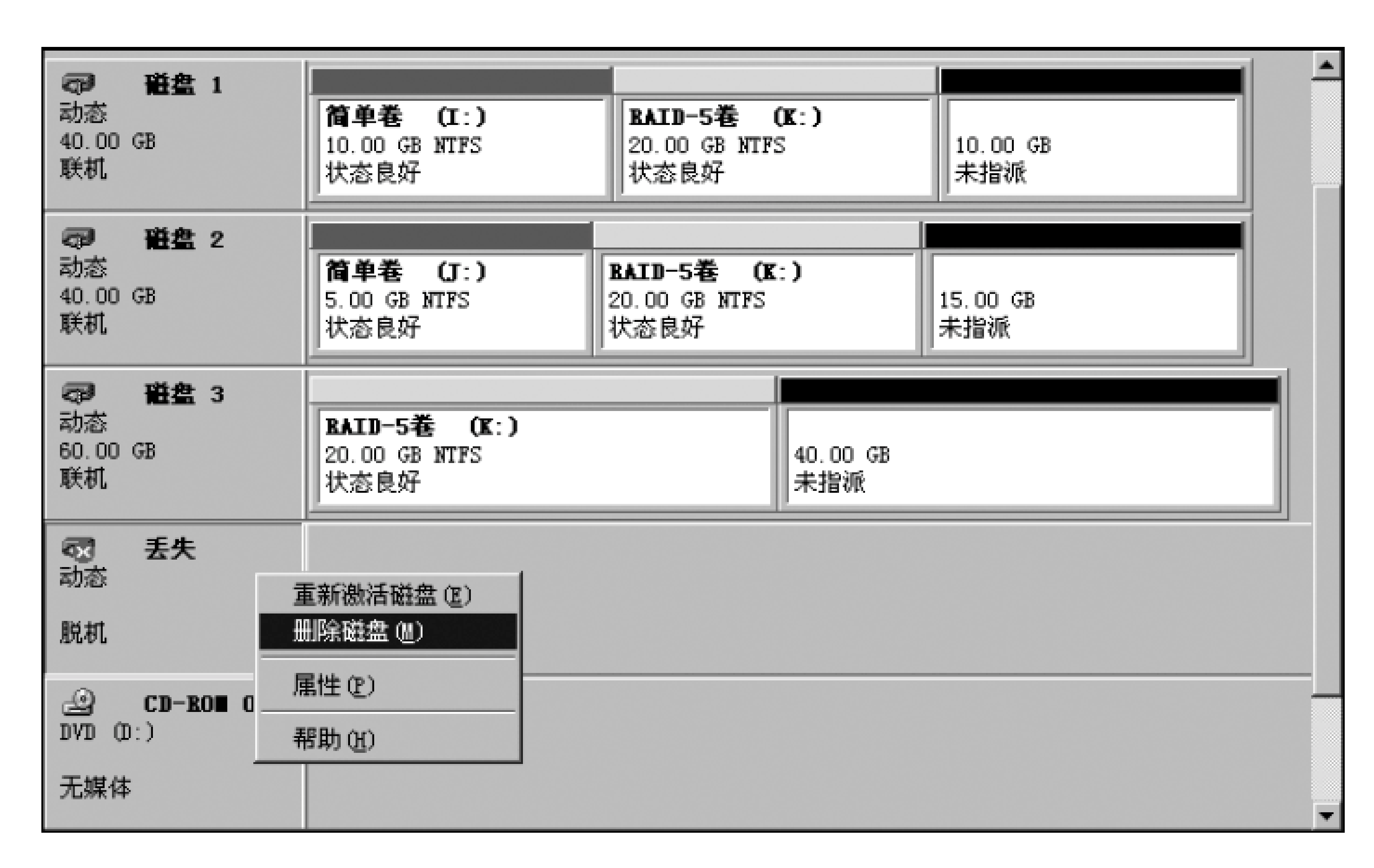


图 3-24 “删除磁盘”命令

2. 删除分区和卷

删除分区和卷的操作步骤如下。

(1) 打开"计算机管理(本地)"控制台,展开"计算机管理(本地)"→"存储"→"磁盘管理"。

(2) 在图形视图或磁盘列表中,右击所要删除的磁盘分区或卷,选择"删除逻辑驱动器"菜单项,在弹出的对话框中,单击"是"按钮即可。

3.5.3 添加新磁盘

如果添加了一块新的磁盘,在重新启动计算机时,系统就会自动检测到这块新磁盘,并且自动更新磁盘系统的状态,这块磁盘也会出现在"磁盘管理"的画面中,而且在运行"磁盘管理"时,系统会自动启动"欢迎使用初始化和转换磁盘向导",以便初始化这块新的磁盘。

如果在"磁盘管理"画面中看不到这块新安装的磁盘,则选择"操作"→"重新扫描磁盘"。

3.5.4 管理驱动器号和路径

1. 管理驱动器号

要更改驱动器号或磁盘路径时,可以右击磁盘分区,选中"更改驱动器号和路径",出现的"更改驱动器号和路径"对话框如图 3-25 所示。

单击"更改"按钮,出现如图 3-26 所示的对话框。

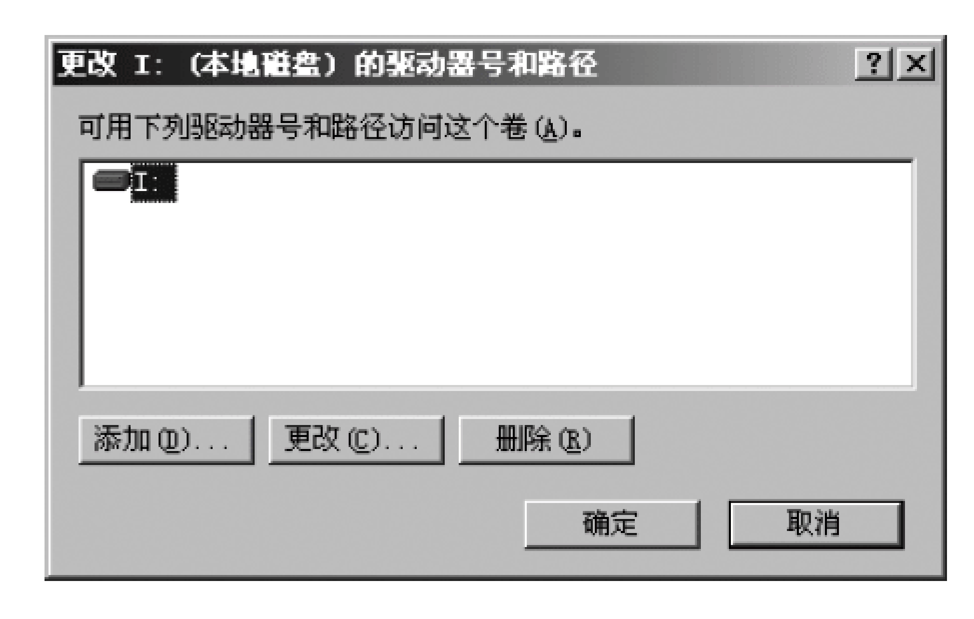


图 3-25 "更改驱动器号和路径"对话框

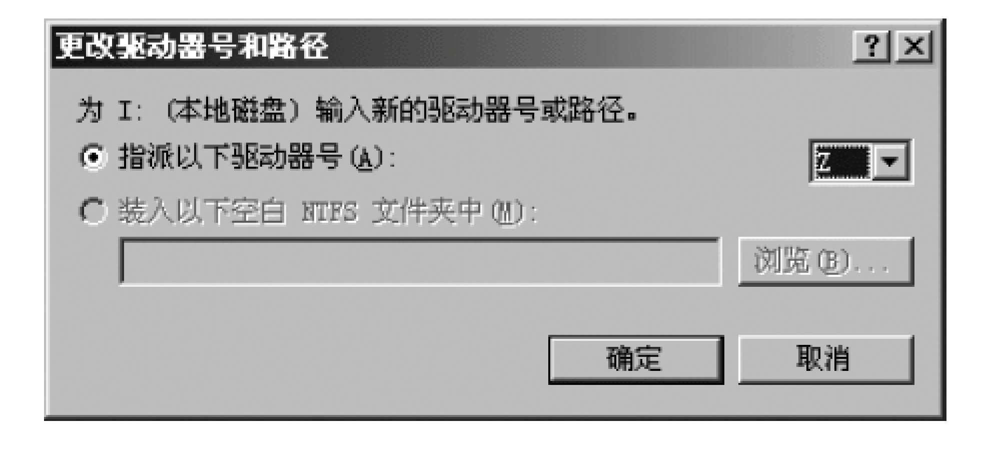


图 3-26 指派驱动器号

指派新的驱动器号为 Z,单击"确定"按钮,如图 3-27 所示。

2. 指派驱动器路径

如果为新建的磁盘分区指派驱动器路径,操作步骤如下。

(1) 在磁盘上选择一个空闲的磁盘分区。右击该磁盘分区,选择"新建逻辑驱动器"

菜单项，如图 3-28 所示。

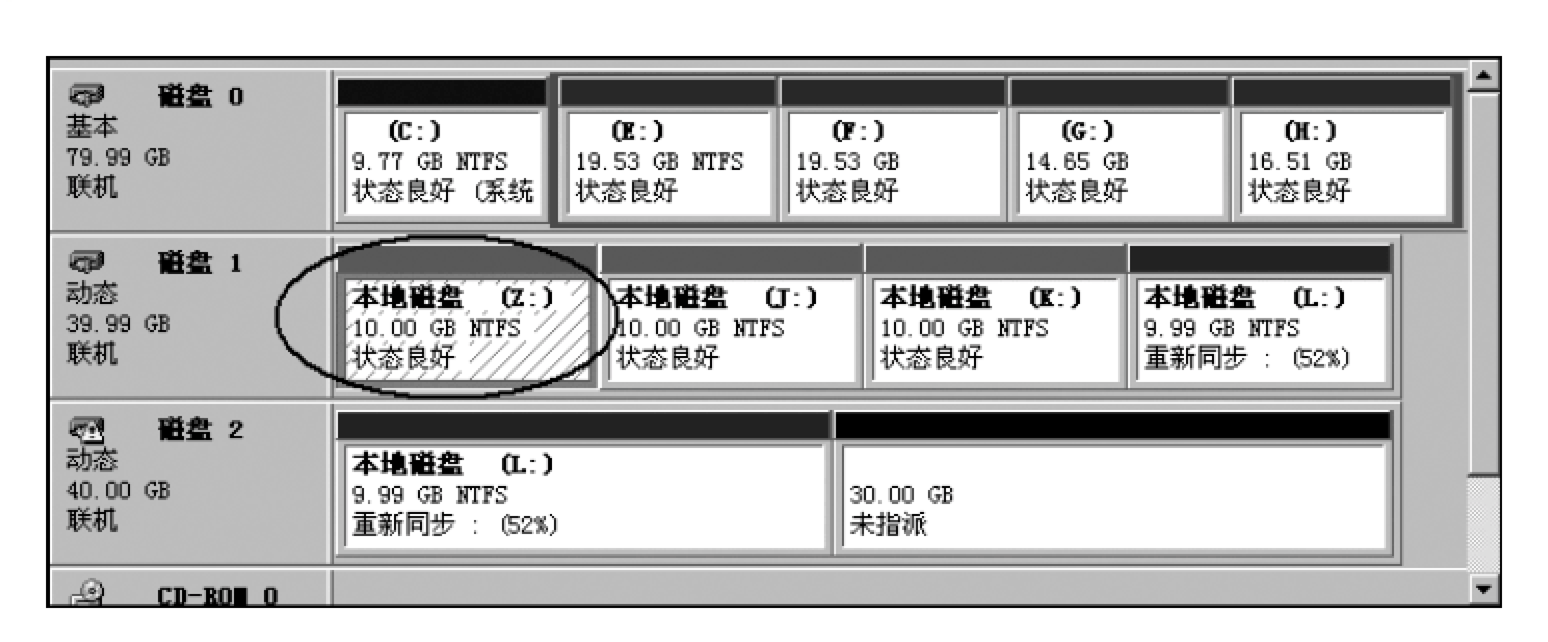


图 3-27　更改后的驱动器号

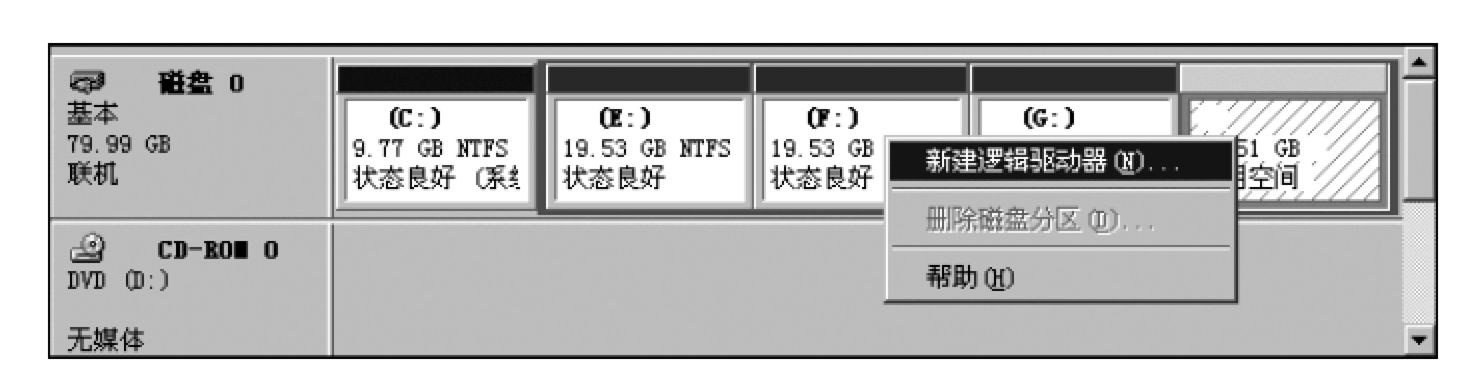


图 3-28　新建逻辑驱动器

（2）在弹出的“新建逻辑驱动器”对话框中，单击“下一步”按钮。弹出“新建磁盘分区向导”对话框，如图 3-29 所示，选择分区类型后，单击“下一步”按钮。

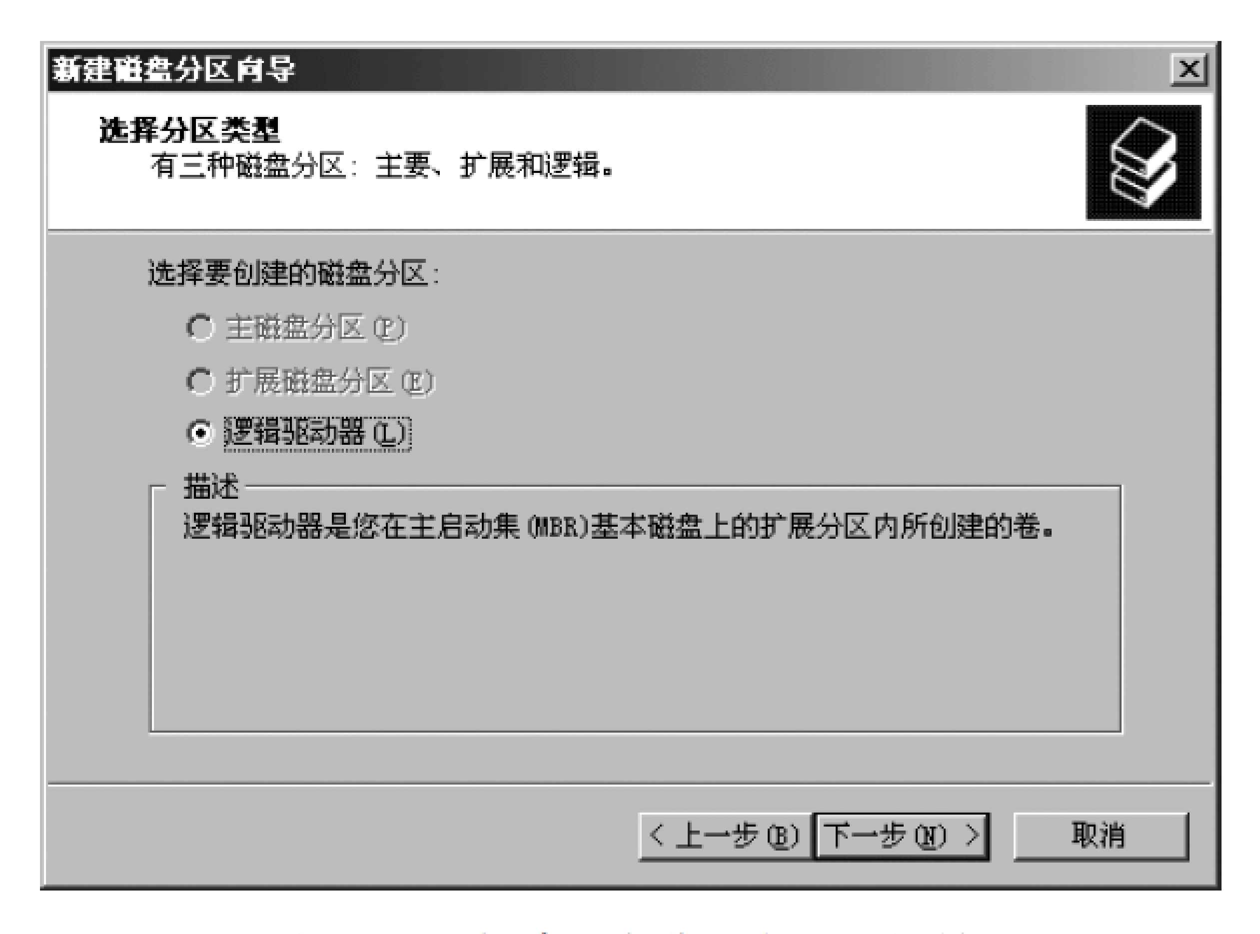


图 3-29　“新建磁盘分区向导”对话框

（3）在弹出的“新建磁盘分区向导”对话框中，为磁盘指定分区大小，单击“下一步”按钮。

（4）在“新建磁盘分区向导”对话框中，指派驱动器号和路径。选择“装入以下空白 NTFS 文件夹中”单选项，如图 3-30 所示，单击“浏览”按钮。

（5）在“浏览驱动器路径”对话框中，在支持驱动器路径的卷中选择一个空文件夹，也可以单击“新建文件夹”按钮在选择的支持驱动器路径的卷中创建一个空白文件夹。创建

完成后的情况如图 3-31 所示，单击“确定”按钮。

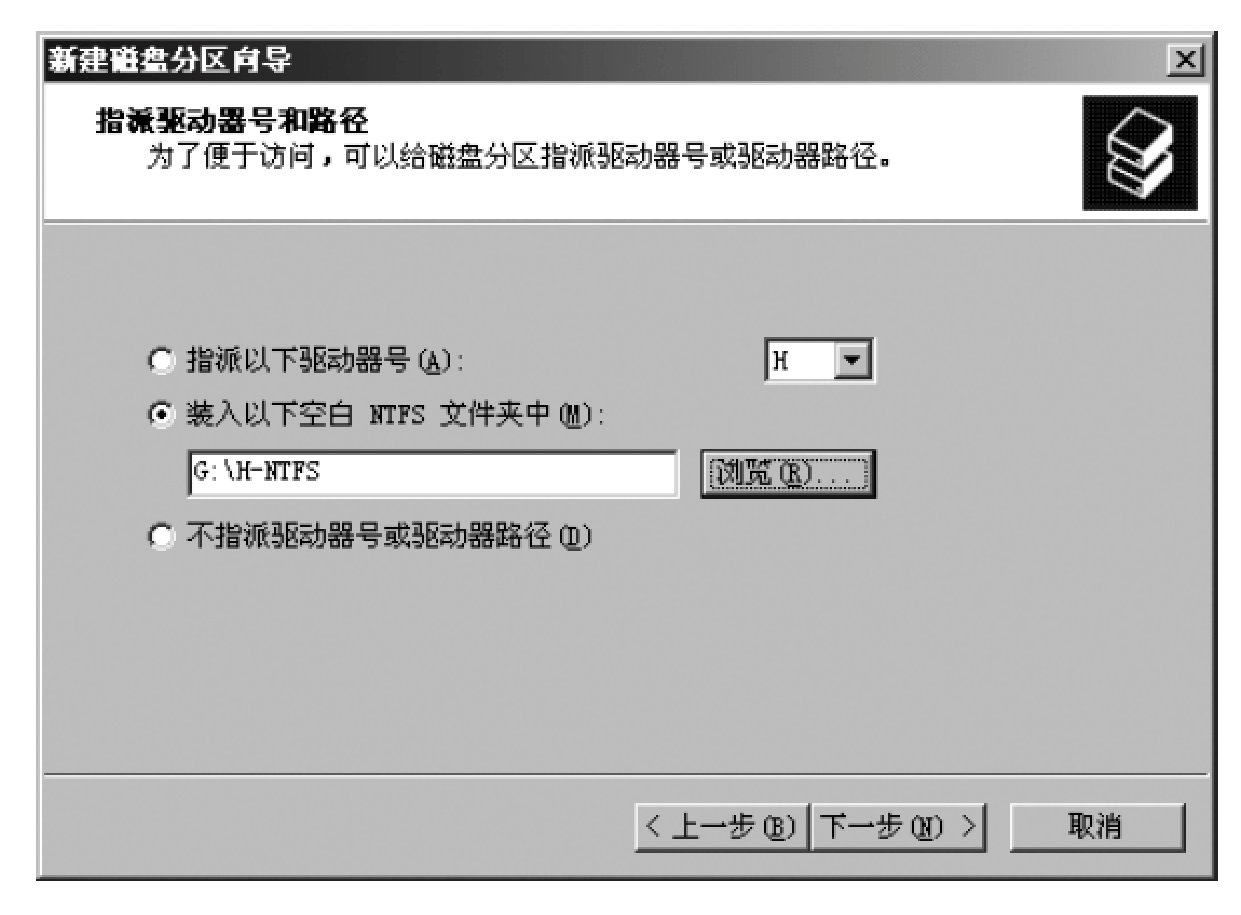


图 3-30　为“新建磁盘分区”指派驱动器号和路径



图 3-31　“浏览驱动器路径”对话框

(6) 在“新建磁盘分区向导”对话框中，指定格式化分区的一些参数设置，如图 3-32 所示。单击“下一步”按钮。

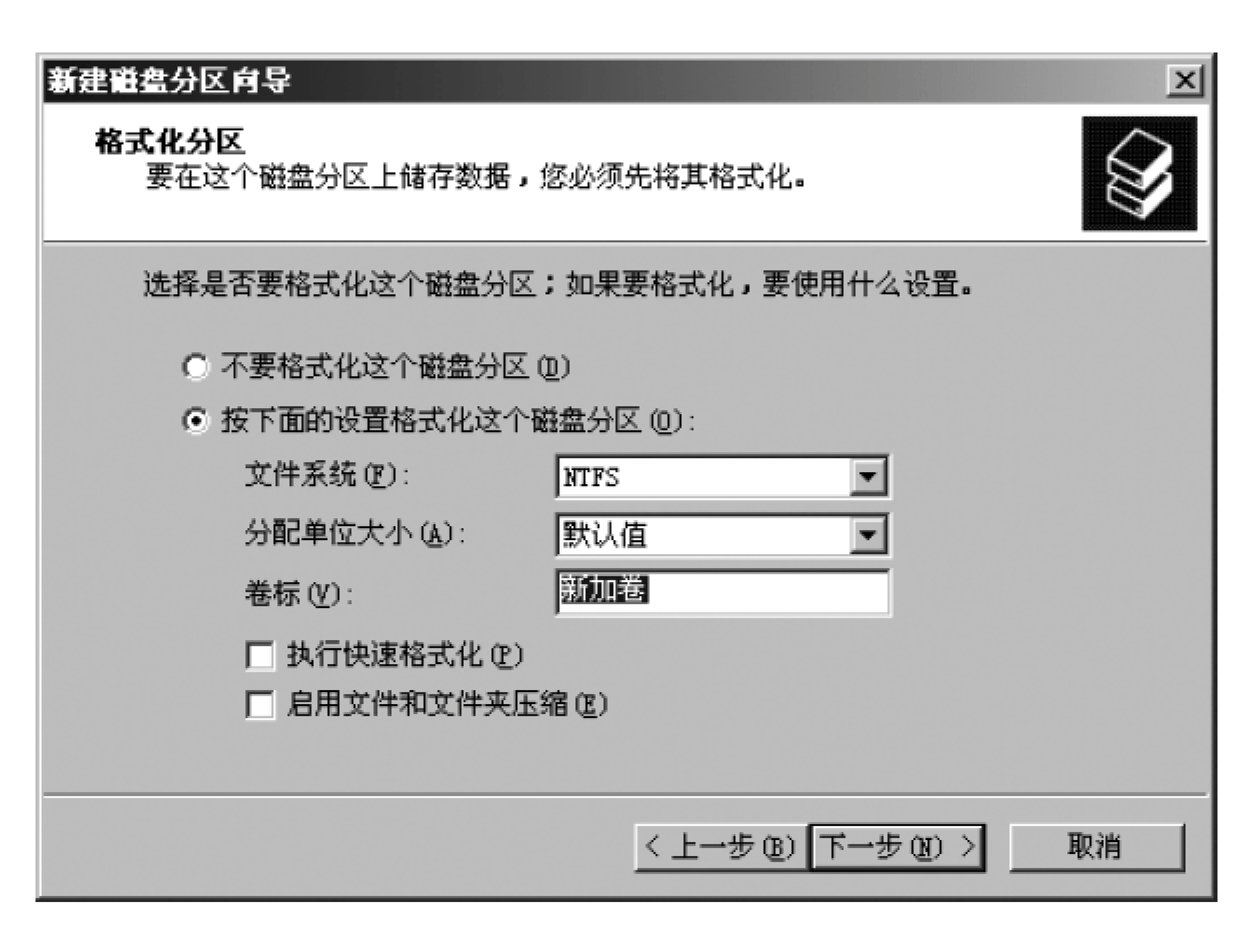


图 3-32　新建磁盘分区格式化设置

（7）在弹出的“新建磁盘分区向导”对话框中，列出了该新建磁盘分区的一些设置，如图 3-33 所示。单击“完成”按钮即可。

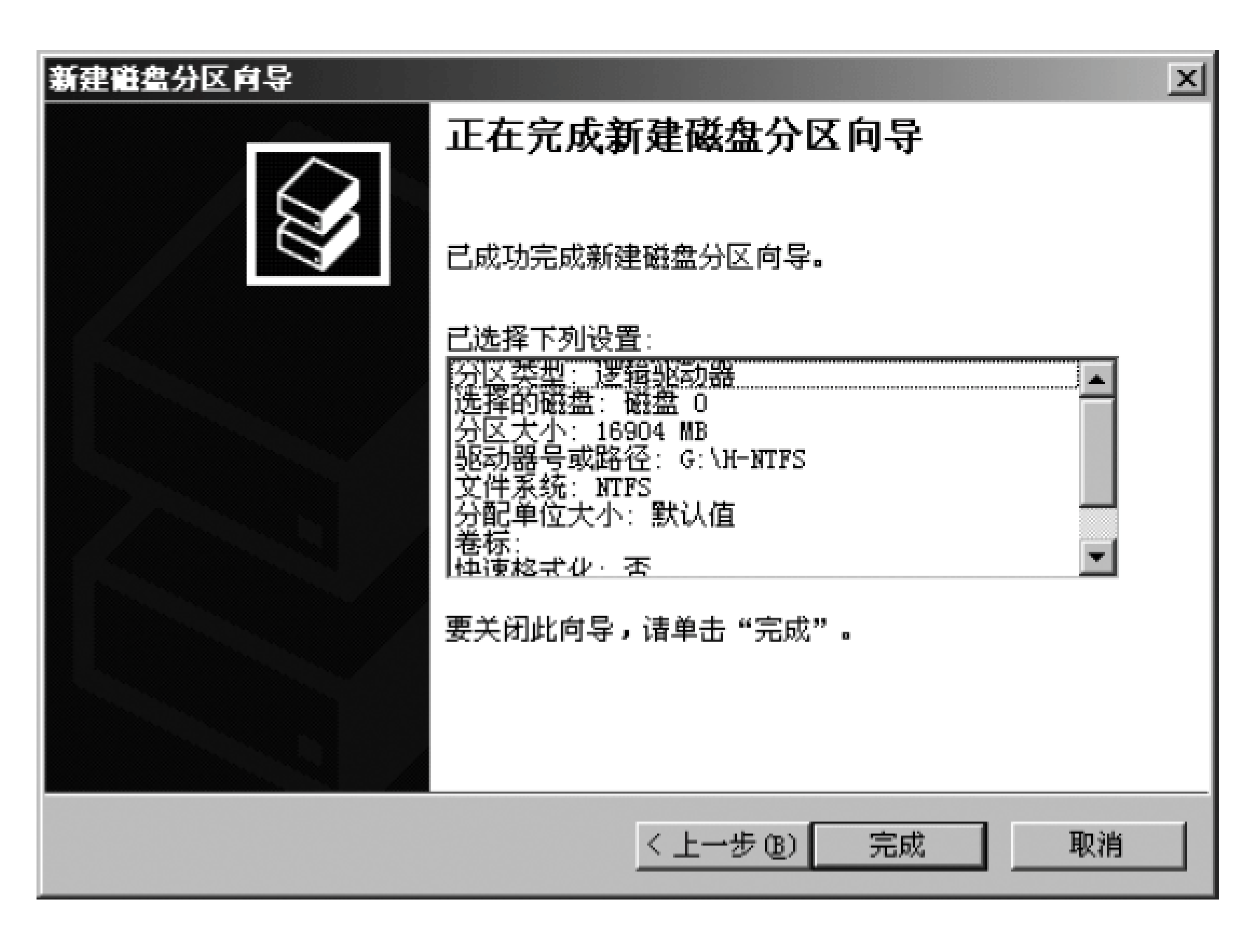


图 3-33 “新建磁盘分区向导”对话框

第 4 章　Active Directory 服务

学习目标

学习完本章后，能够了解 Active Directory 的概念、功能以及 Active Directory 对象的类型，掌握如何配置网络中的域控制器，理解 Active Directory 的逻辑结构(域、组织单位、目录树、目录林和信任)、物理结构(域控制器、站点)，掌握在 Active Directory 中发布资源的方法。

4.1　Active Directory 概述

Windows Server 2003 网络中提供的 Active Directory 服务构建了网络资源的架构，提供了组织、管理和访问这些网络资源(例如用户、计算机、共享文件夹和打印机等)的功能，还提供了集中管理 Windows Server 2003 网络的功能，这意味着管理员可以在某个位置集中管理整个网络。Active Directory 还支持管理员对 Active Directory 对象进行控制委派管理，这使得管理员能将对 Active Directory 对象或属性的管理权限分配给某个特定的用户组。

Active Directory 存储了整个网络的资源信息，并简化了用户查找、管理和访问这些网络资源的操作，这些网络资源包括用户、计算机、共享文件夹和打印机等。

4.1.1　Active Directory 概念

本书中的 Active Directory 是指 Windows Server 2003 网络中的目录服务。目录服务用于存储网络资源信息并使用户和应用程序能够访问这些资源。目录服务提供了统一的命名、描述、查找、访问和管理网络资源的方法，还为网络资源提供了安全保障。

Active Directory 使得网络的拓扑结构和协议对用户是透明的，从而使网络上的用户只需要一个单一的账户就可以访问任何资源(例如打印机)，而无须知道该资源的位置以及它是如何连接到网络的。Active Directory 允许用户只登录一次就能够访问在 Active Directory 上的所有资源。

Active Directory 被划分成区域进行管理，这使其可以存储大量的对象。基于这种结构，Active Directory 可以随着企业规模的扩大而扩展。

Active Directory 支持集中式管理。可以将系统配置信息、应用程序信息和用户配置文件的位置信息存储在 Active Directory 中。当与组策略结合使用时，Active Directory 使管理员能够从网络的核心位置使用统一的管理界面对分布于各处的成员计算机、网络服务和应用程序进行管理。

4.1.2 Active Directory 对象

Active Directory 对象表示网络中的资源,这些资源包括用户(组)、计算机、共享文件夹和打印机等。网络中所有的服务器、域和站点也可以被看作对象。

当创建对象时,用于描述对象特征的属性信息将被存储在活动目录中,例如,用于描述用户对象的属性有用户登录名称、姓、名、电话、电子邮件等。通过指定对象的具体属性,可以在 Active Directory 查找到相应的对象。例如,可以通过指定用户对象的"用户登录名称"属性来查找符合条件的用户。

Active Directory 中的某些特定对象(例如域、容器和组织单位)可以包含其他对象。可以将这些域、容器和组织单位组织成一个结构层次,而那些代表网络资源的对象,例如用户、计算机、组、共享文件夹和打印机等,则根据其不同的管理方式放入相应的结构层次中。

表 4-1 列出了一些最常用的 Active Directory 对象。

表 4-1　常用的 Active Directory 对象

对象类型	描　　述
用户	包含域内用户信息的对象,包含用户登录名、密码等信息,还包含可选字段,如姓、名、显示名称、电话号码、电子邮件和网页等
联系人	与企业有联系的人员,包含可选字段,如电话号码、电子邮件、地址和主页等信息
组	包含一组用户、计算机和\或其他组对象的对象,使用该对象可以简化管理
共享文件夹	指向计算机上共享文件夹的指针对象,包含数据的位置而不是数据本身。在 Active Directory 中发布共享文件夹的同时,创建了一个指向该共享文件夹的指针对象
打印机	指向计算机上打印机的指针对象。如果计算机不是域的成员,则必须手工发布该计算机上的打印机。在域中计算机上安装的打印机会自动到发布到 Active Directory 中
计算机	包含域内计算机信息的对象
域控制器	包含域控制器信息的对象,包括一些可选描述信息,如 DNS 名、Windows Server 2000 以前版本的计算机名、操作系统版本、域控制器位置和管理者的信息等
组织单位	包含其他对象(如用户、组、计算机和其他组织单位)的容器对象。使用组织单位(OU)可以在 Active Directory 中建立层次结构

4.2 配置域控制器

如果要构建域结构的 Windows Server 2003 网络,则网络上必须有域控制器。域控制器是一台运行 Windows Server 2003 并存储 Active Directory 的计算机。域控制器通过 Active Directory 提供目录服务,例如负责维护 Active Directory 数据库、验证用户的账户与密码是否正确、将 Active Directory 数据库复制到其他的域控制器。

一个域内可以有多台域控制器。多台域控制器可以提供足够的功能和容错功能,即使一台域控制器出现故障,仍然能够由其他域控制器提供服务。多台域控制器还可以平

衡用户登录的负担,改善用户登录的效率。

为了简单起见,本节仅介绍如何创建整个域目录林中的第一个域(根域)。假设域的名称为 xyz. net,并在该域中设置两台域控制器,即 server01. xyz. net 和额外的域控制器 server02. xyz. net。域目录林和域树的结构如图 4-1 所示。这种网络环境已经能够满足一个小型企业的需求。而对于分布于不同地理位置的大型企业,通常需要在每个位置配置一个或多个域控制器才能够提供足够的功能和容错能力。

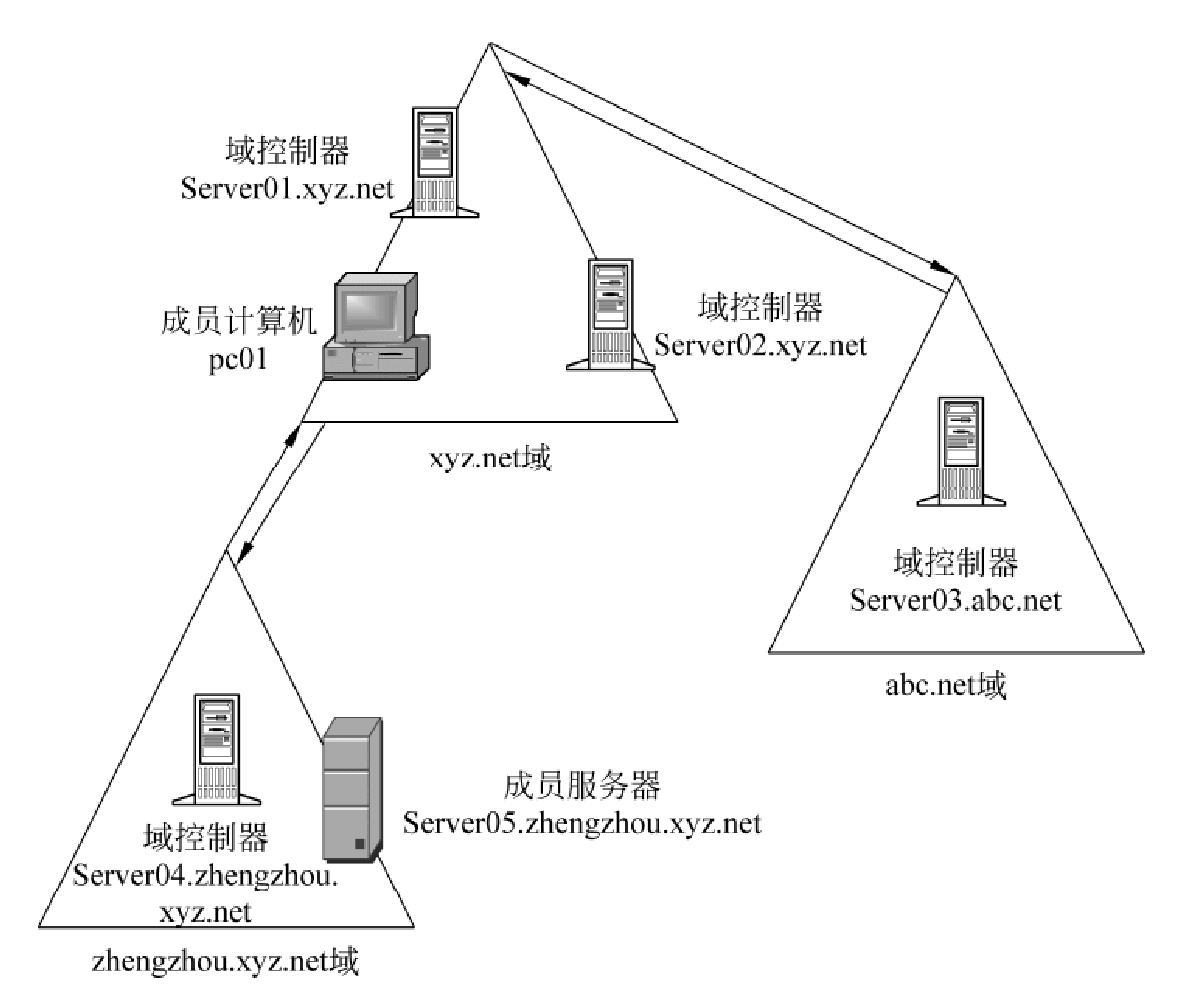


图 4-1 域目录林和域树的结构

4.2.1 创建域的必要条件

将一台独立服务器或成员服务器(已安装 Windows Server 2003 标准版、企业版或 Datacenter 版操作系统)升级为域控制器,就是在这台服务器上安装活动目录。在升级之前,请先检查以下工作是否准备就绪。

(1) DNS 域名。Windows Server 2003 域名采用 DNS 的结构与命名方式,因此必须为域指定一个符合 DNS 规格的域名(例如 xyz. net)。

(2) DNS 服务器。在 Windows Server 2003 域结构的网络中,域控制器会将自己登记到 DNS 服务器内,以便让其他计算机通过 DNS 服务器查找到这台域控制器,因此网络中必须有一台 DNS 服务器,而这台 DNS 服务器必须支持“服务位置资源记录”(Server Location Resource Record, SRV RR)与“动态更新”的功能。如果网络中目前还没有支持服务器位置资源记录与“动态更新”的 DNS 服务器,则可以在将独立服务器或成员服务器升级为域控制器时,同时安装 DNS 服务。

(3) NTFS 磁盘分区。域控制器需要一个能够提供安全设置的磁盘分区,用于存储 SYSVOL 文件夹(SYSVOL 文件夹内存储着诸如登录、注销、启动和关闭脚本以及与组策略有关的数据)。

4.2.2 创建第一台域控制器

下面介绍如何创建如图 4-1 所示的根域为 xyz. net 的域目录树,并创建第一台域控制器 Server01. xyz. net。

在创建网络中的第一台域控制器(例如 server01. xyz. net)时,就会同时创建该域控制器所隶属的域(例如 xyz. net),同时还会创建该域所隶属的域目录树,而该域就是这个域目录树的根域。由于这是第一个域目录树,因此还会同时创建一个新的域目录林,这个域目录林的名称就是第一个域目录树的根域的域名,也就是 xyz. net。域 xyz. net 也就是整个域目录林的"目录林根域"。

可以通过以下两种方法创建网络中的第一台域控制器。

(1) 利用 Active Directory 安装向导。它会以完整的步骤指导用户安装活动目录。

(2) 典型配置。这种配置方法适合于配置网络内的第一台服务器。

1. 利用 Active Directory 安装向导

创建网络中的第一台域控制器,操作步骤如下。

(1) 通过以下 3 种方法启动"Active Directory 安装向导"。

① 选择"开始"→"运行",在"运行"对话框中输入 dcpromo。

② 选择"开始"→"管理工具"→"配置您的服务器向导"→"自定义配置"→"域控制器(Active Directory)",单击"下一步"按钮。

③ 选择"开始"→"管理工具"→"管理您的服务器"→"添加或删除角色"→"自定义配置"→"域控制器(Active Directory)",单击"下一步"按钮。

(2) 出现"欢迎使用 Active Directory 安装向导"对话框,单击"下一步"按钮。

(3) 出现"操作系统兼容性"对话框,提示以前版本的 Windows,例如 Windows 95 与 Windows NT 4.0 SP3 或更早的版本,默认将无法登录到运行 Windows Server 2003 的域控制器或访问域资源,单击"下一步"按钮。

(4) 在"域控制器类型"、"创建一个新域"对话框中,分别选择"新域的域控制器"、"在新林中的域",如图 4-2 所示,单击"下一步"按钮。

(5) 如果出现如图 4-3 所示的对话框,表示目前没有为这台计算机指定首选 DNS 服务器,否则直接转到步骤(6)。

① 如果网络上已有支持活动目录的 DNS 服务器,则选择"是,将配置 DNS 客户端"。单击"下一步"按钮,为本机配置"首选 DNS 服务器"后,再继续后续的操作。

② 如果要在这台计算机上安装并配置 DNS 服务,则选择"否,只在这台计算机上安装并配置 DNS"。在此选择此项,即在这台计算机上安装 DNS 服务。



图 4-2　指定域控制器类型和域的类型

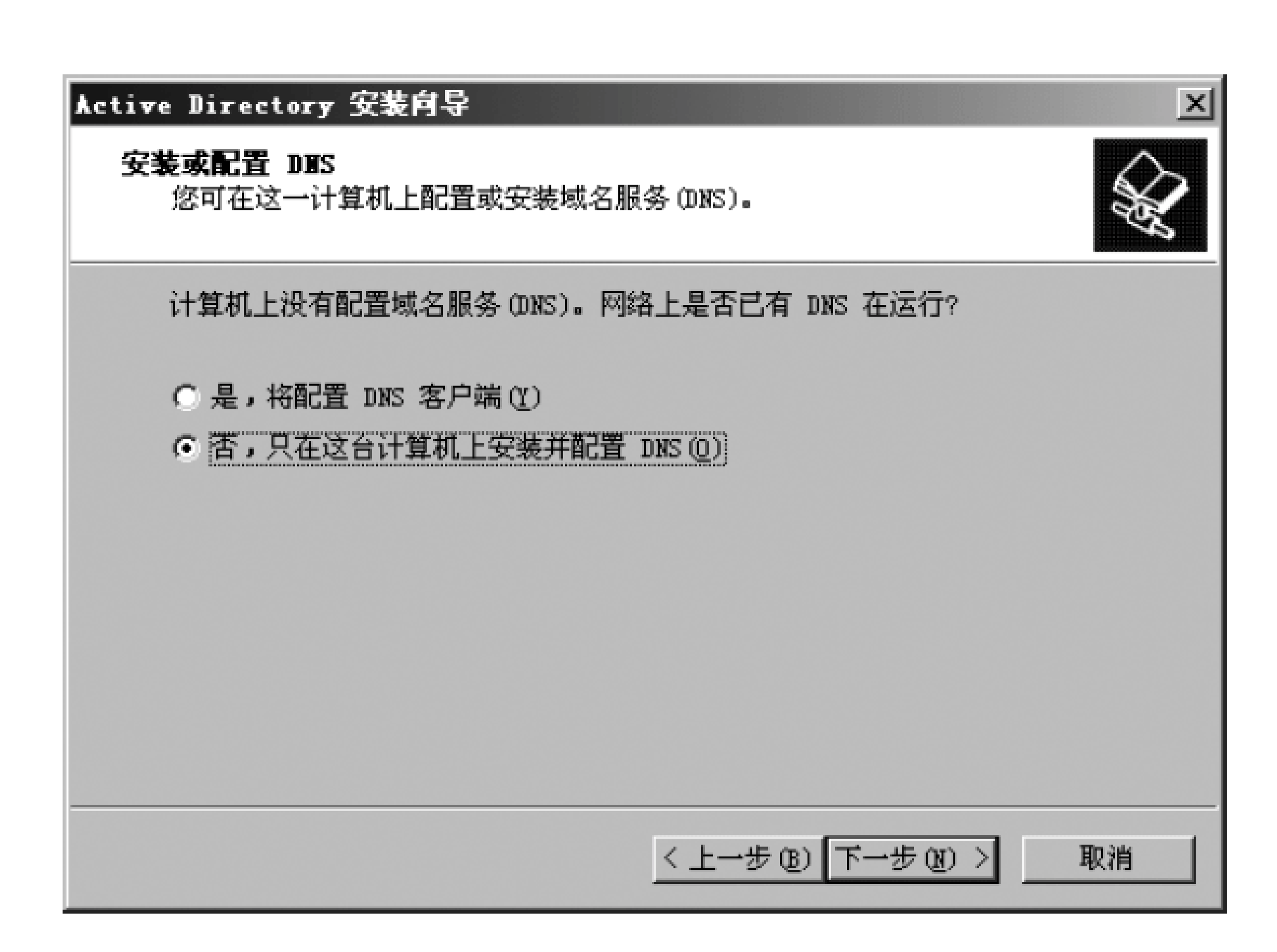


图 4-3　安装或配置 DNS

(6) 在如图 4-4 所示的对话框中输入新域的 DNS 全名(例如 xyz.net)，接下来安装程序会花一些时间来检查该域名是否已经存在，如果已存在，安装程序会要求重新设置一个域名。

(7) 在 NetBIOS 域名对话框中，指定新域的 NetBIOS 名称。这个名称是早期 Windows 版本的用户用来识别新域的。如果 DNS 域名为 xyz.net，则默认的 NetBIOS 域名为 XYZ。单击“下一步”按钮，接受默认的名称，也可以输入新名称，在此保留默认的名称。

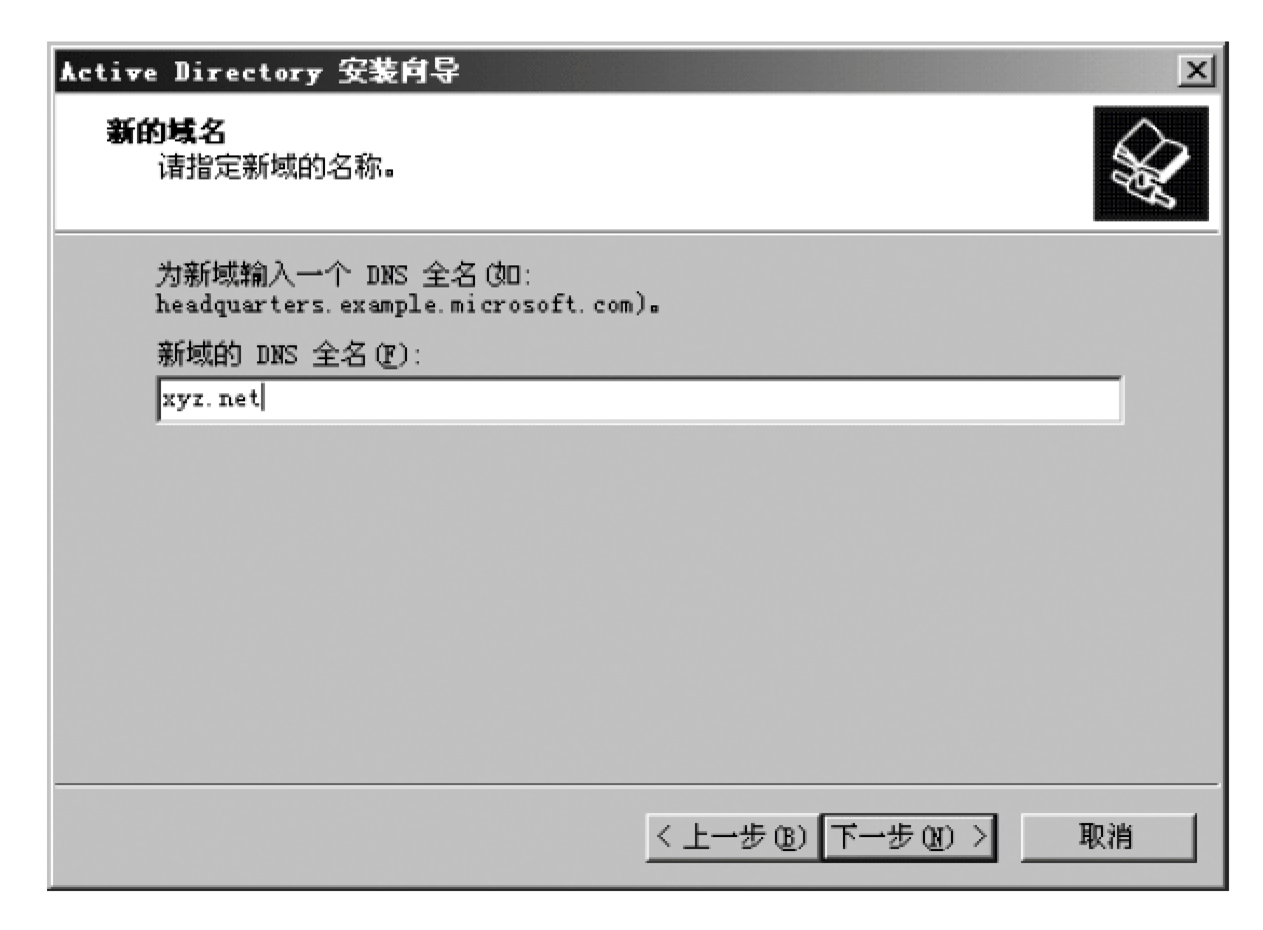


图 4-4　指定新域的名称

(8) 在“数据库和日志文件文件夹”对话框中,指定 Active Directory 数据库文件夹和日志文件夹的位置。数据库文件夹用来存储活动目录数据库,日志文件夹用来存储活动目录的日志,该日志可以用来修复活动目录,单击“下一步”按钮使用默认值。

(9) 在“共享的系统卷”对话框中,指定 SYSVOL 文件夹的位置。该文件夹存储与组策略相关的数据,必须位于 NTFS 卷上,单击“下一步”按钮使用默认位置 C:\WINDOWS\SYSVOL。

(10) 如果出现如图 4-5,表示为这台计算机配置的首选或备用 DNS 服务器都没有响应或者没有负责该域的区域(例如负责 xyz.net 域的区域),或者不支持活动目录(例如不支持 SRV 或动态更新)。此时,可以直接选择第二个选项,或者参阅以下的说明后再选择合适的选项。否则,请直接转到步骤(11)。

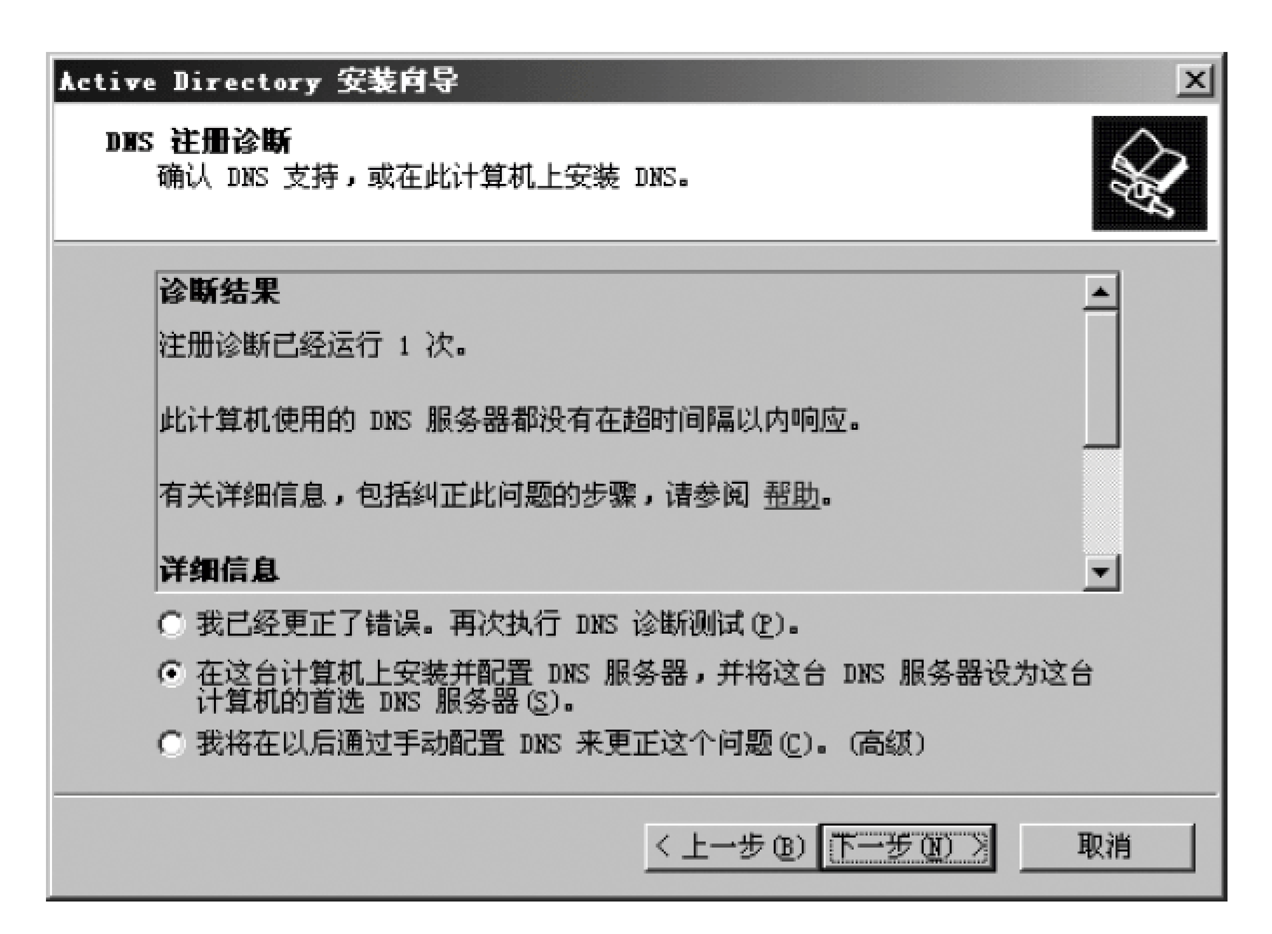


图 4-5　DNS 注册诊断

① 可以暂时停止操作,先去解决 DNS 服务器的问题,完成后再选择第 1 项。

② 如果要在这台计算机上安装并配置 DNS 服务器,并将这台 DNS 服务器设为这台

计算机的"首选 DNS 服务器"，则选择第 2 项。

③ 用户也可以选择"我将在以后通过手动配置 DNS 来更正这个问题"单选项，建议尽快解决 DNS 服务器的问题，否则域将无法正常工作。

(11) 在图 4-6 中，单击"下一步"按钮，或者参阅以下说明后再选择合适的选项。

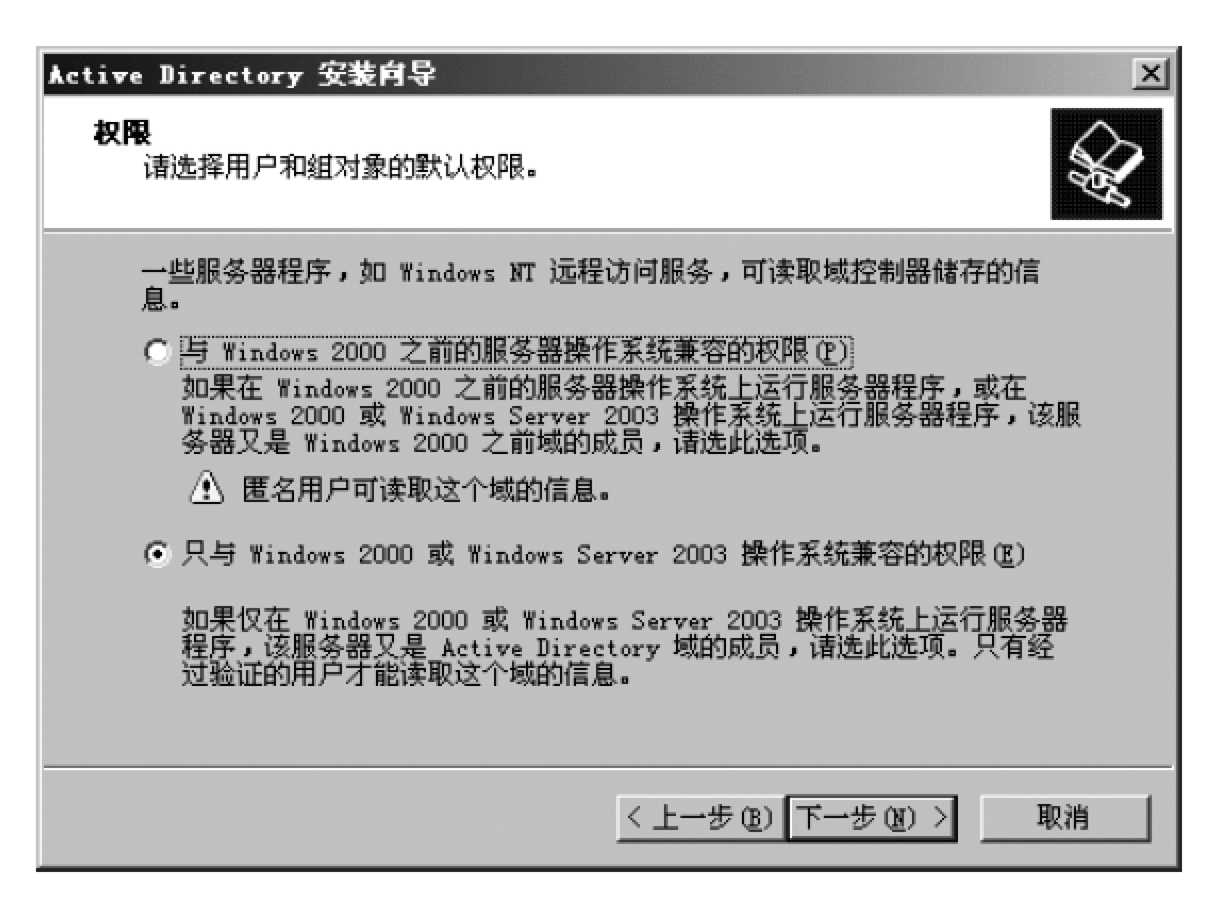


图 4-6 选择用户和组的默认权限

① "与 Windows 2000 之前的服务器操作系统兼容的权限"。如果在 Windows NT Server 或者 Windows 2000 Server/Windows Server 2003(隶属于 Windows NT 域)上运行一些服务器程序时，则选择该选项，该选项允许匿名用户 Anonymous 读取这个域的信息。

② "只与 Windows 2000 或 Windows Server 2003"操作系统兼容的权限。如果仅在隶属于活动目录域内的 Windows 2000 或 Windows Server 2003 计算机上运行所有服务器程序，则选择该选项，该选项只允许经过身份验证的用户访问这个域的信息。

(12) 在图 4-7 中输入"目录服务还原模式"的管理员密码。可以在计算机启动时按 F8 键进入"目录服务还原模式"，输入此处所设置的密码，成功进入该模式后可以修复活动目录数据库。

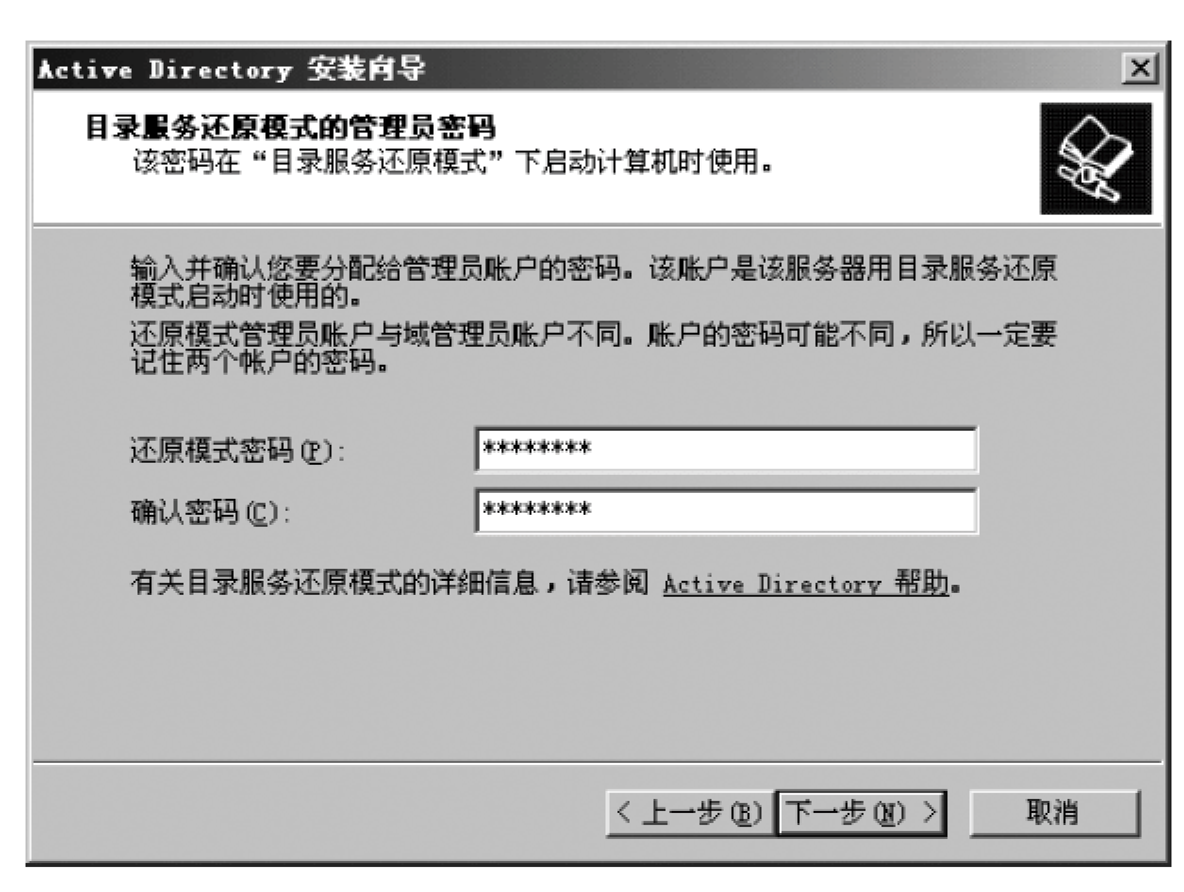


图 4-7 指定目录服务还原模式的管理员密码

提示："目录服务还原模式"的管理员账户与域管理员账户不同，其密码也可以设为不同。

(13) 确认各项设置无误后，如图 4-8 所示，单击"下一步"按钮。

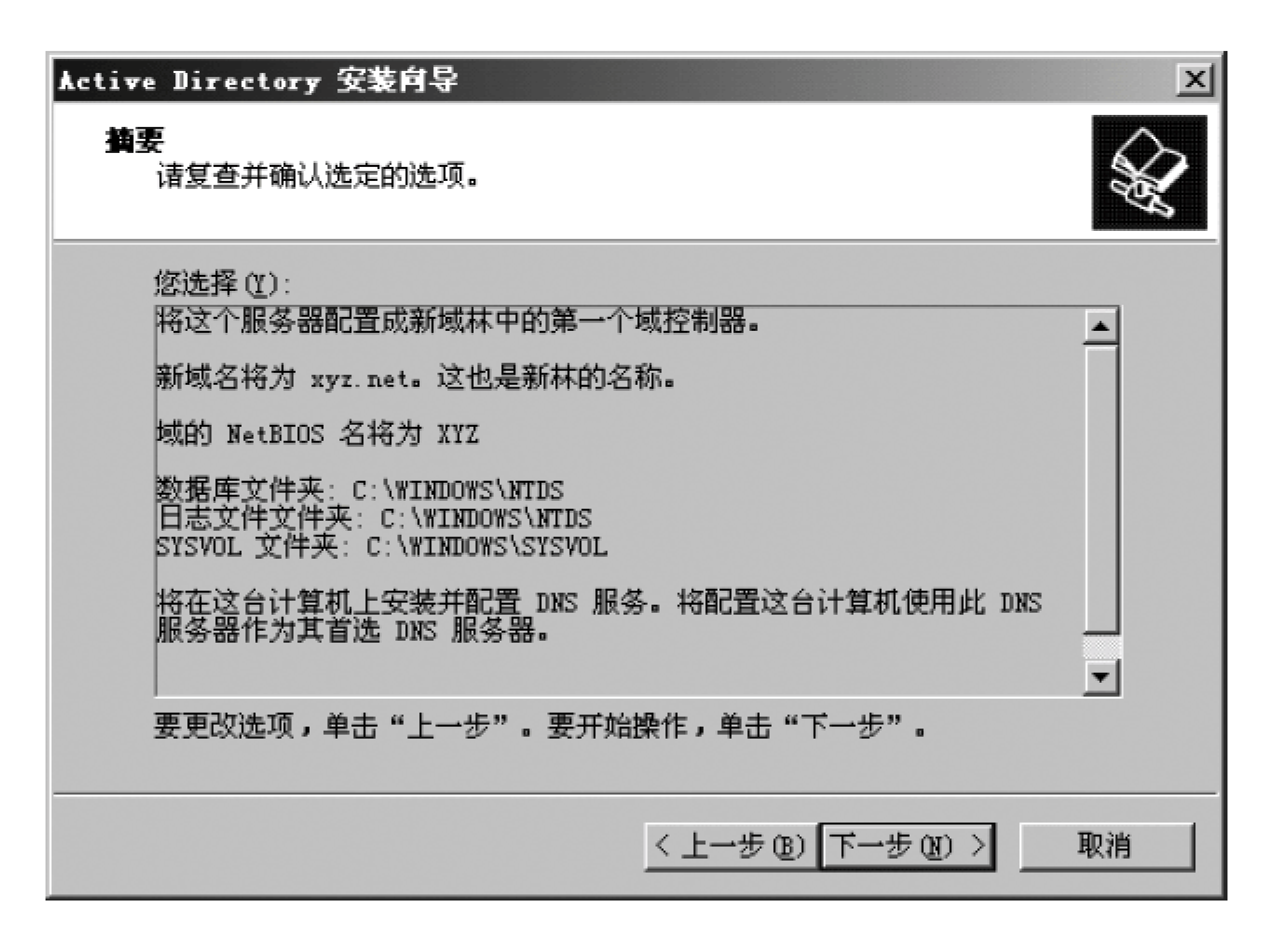


图 4-8　复查并确认选项

(14) 接下来，系统会花一些时间安装活动目录，之后，在"正在完成 Active Directory 安装向导"对话框中，单击"完成"按钮。出现如图 4-9 所示的信息提示对话框时，单击"立即重新启动"按钮，重新启动 Windows，至此域控制器安装完成。



图 4-9　"信息提示"对话框

2. 典型配置

典型配置适合于配置网络内的第一台服务器，而且是唯一的一台服务器。典型配置的操作步骤如下。

(1) 在 Windows Server 2003 独立服务器上，通过以下两种方法启动"配置您的服务器向导"。

① 单击"开始"→"管理工具"→"配置您的服务器向导"，出现"欢迎使用配置您的服务器向导"，单击"下一步"按钮。

② 单击"开始"→"管理工具"→"管理您的服务器"，单击"添加或删除角色"。

(2) 出现图 4-10 时，检查列举的这些预备步骤是否已经完成，例如网卡是否安装/配置正确、线缆是否连接好、安装 CD 是否准备就绪等。确认完成后，单击"下一步"按钮。

(3) 在图 4-11 中，选择"第一台服务器的典型配置"，该选项会在这台计算机上同时安装活动目录服务、DNS 服务、DHCP 服务(如果需要)。



图 4-10　预备步骤

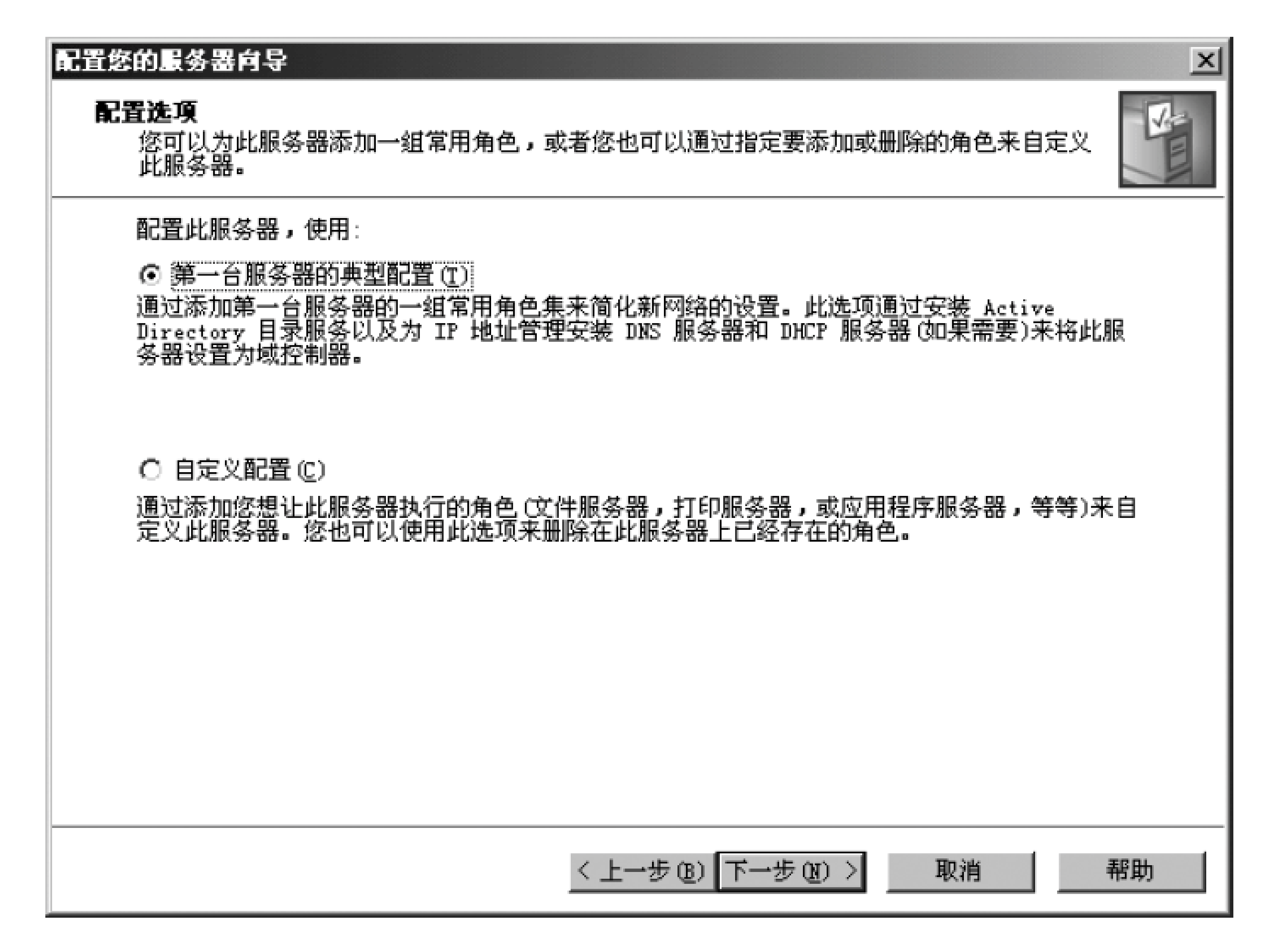


图 4-11　指定服务器配置选项

提示：如果网络上已经有一台 DHCP 服务器，并且支持该网络的作用域，则不会出现如图 4-11 所示的对话框，而是直接进入图 4-12，此时需要选择“域控制器(Active Directory)”，然后利用“Active Directory 安装向导”，再将计算机升级为域控制器。

(4) 在图 4-13 中，输入新域的 DNS 全名(例如 xyz. net)。完成后，单击“下一步”按钮。

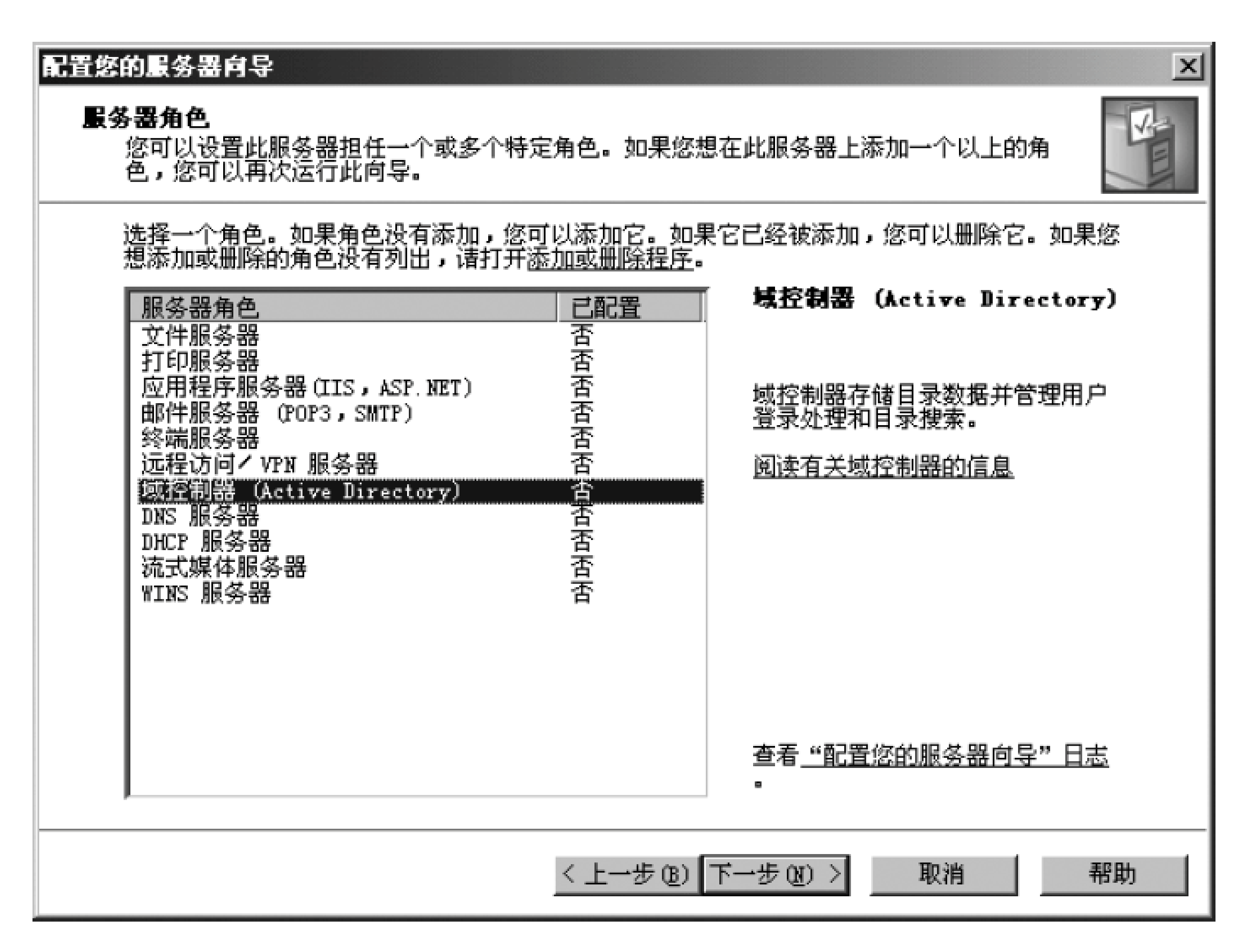


图 4-12 指定服务器角色

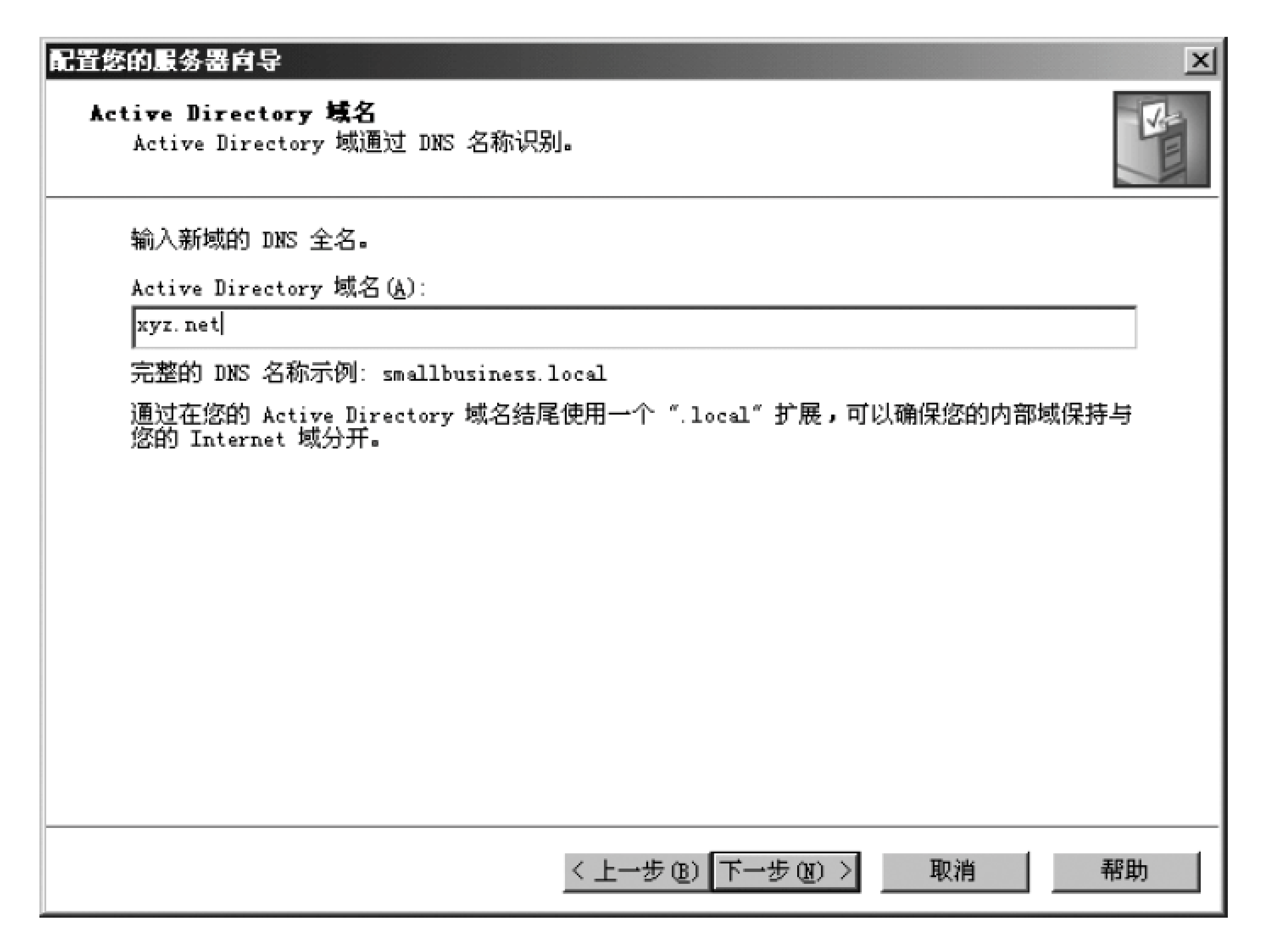


图 4-13 指定 Active Directory 域名

(5) 在图 4-14 中，默认显示一个由 DNS 域名派生的 NetBIOS 域名，例如，如果 DNS 域名为 xyz.net，则默认的 NetBIOS 域名就是 XYZ。可以更改该名称，完成后，单击"下一步"按钮。

(6) 如果没有为这台服务器配置首选或备用 DNS 服务器，则出现图 4-15。此时，如果用户知道扮演转发器(转发器是另外一台 DNS 服务器，可以解析此 DNS 服务器不能解析的 DNS 查询)的 DNS 服务器的 IP 地址，请选择"是，将查询转发到 IP 地址如下的 DNS 服务器"，然后输入 IP 地址，否则选择"否，不转发查询"。

配置您的服务器向导
NetBIOS 名
运行非 Windows 2000，Windows XP 和 Windows Server 2003 家族的客户端将使用 NetBIOS 域名。
默认 NetBIOS 名称由 DNS 域名派生。
DNS 域名：
xyz.net
要更改默认 NetBIOS 名称，请在下面的框中输入新的名称。
NetBIOS 域名(E)：
XYZ
< 上一步(B) 下一步(N) > 取消 帮助

图 4-14　指定域的 NetBIOS 名

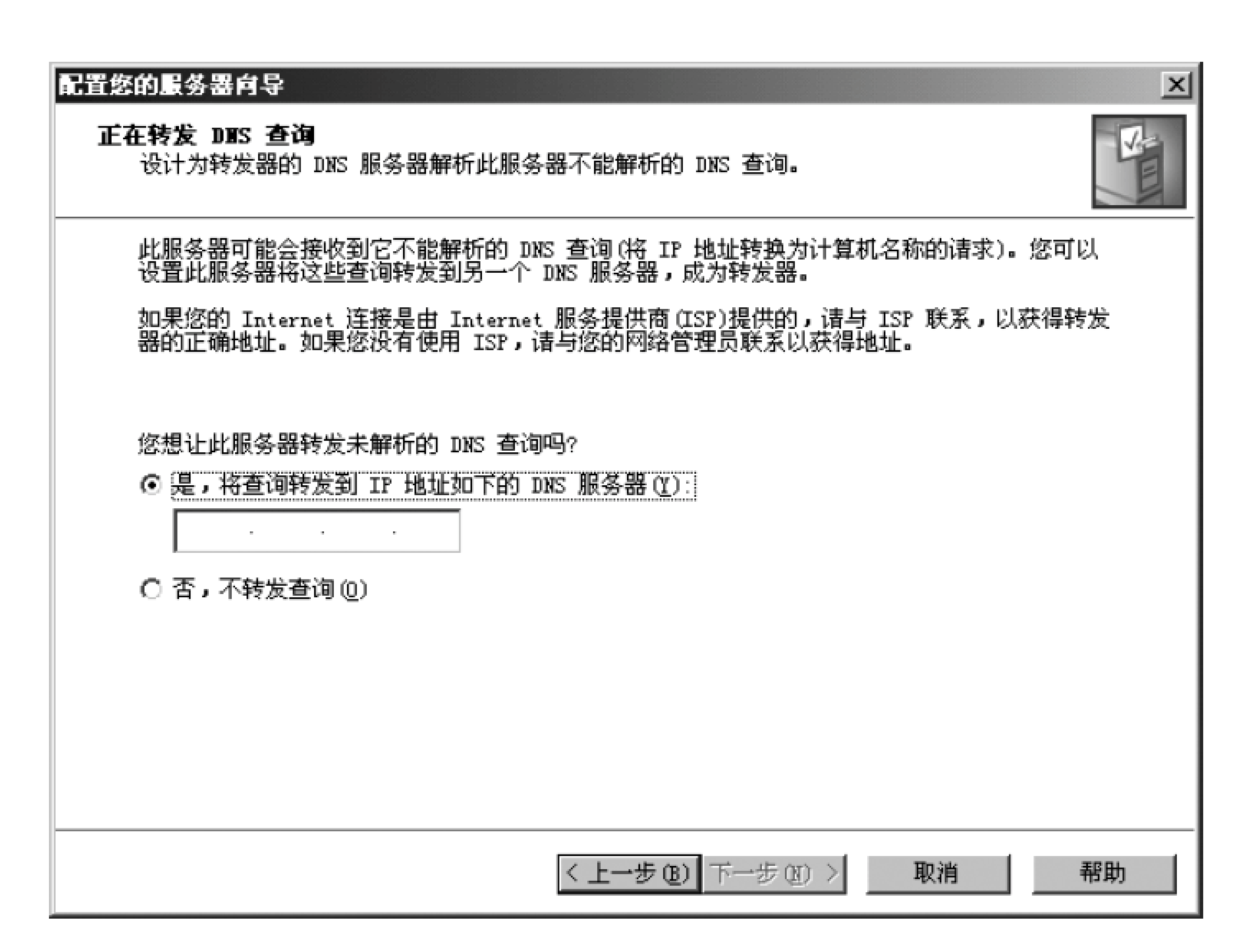


图 4-15　指定转发查询

如果已经为这台计算机配置了“首选 DNS 服务器”，则向导会自动将该 DNS 服务器设置为“转发器”，而且会直接转到步骤(7)。

(7) 出现图 4-16 时，单击“下一步”按钮。

(8) 出现图 4-17 时，在关闭所有打开的程序后，单击“确定”按钮。

(9) 在安装过程中，系统会提示插入 Windows Server 2003 安装光盘，插入光盘后，单击“确定”按钮。接下来，系统会花一些时间安装并配置 DHCP 服务器、活动目录和 DNS 服务器等。

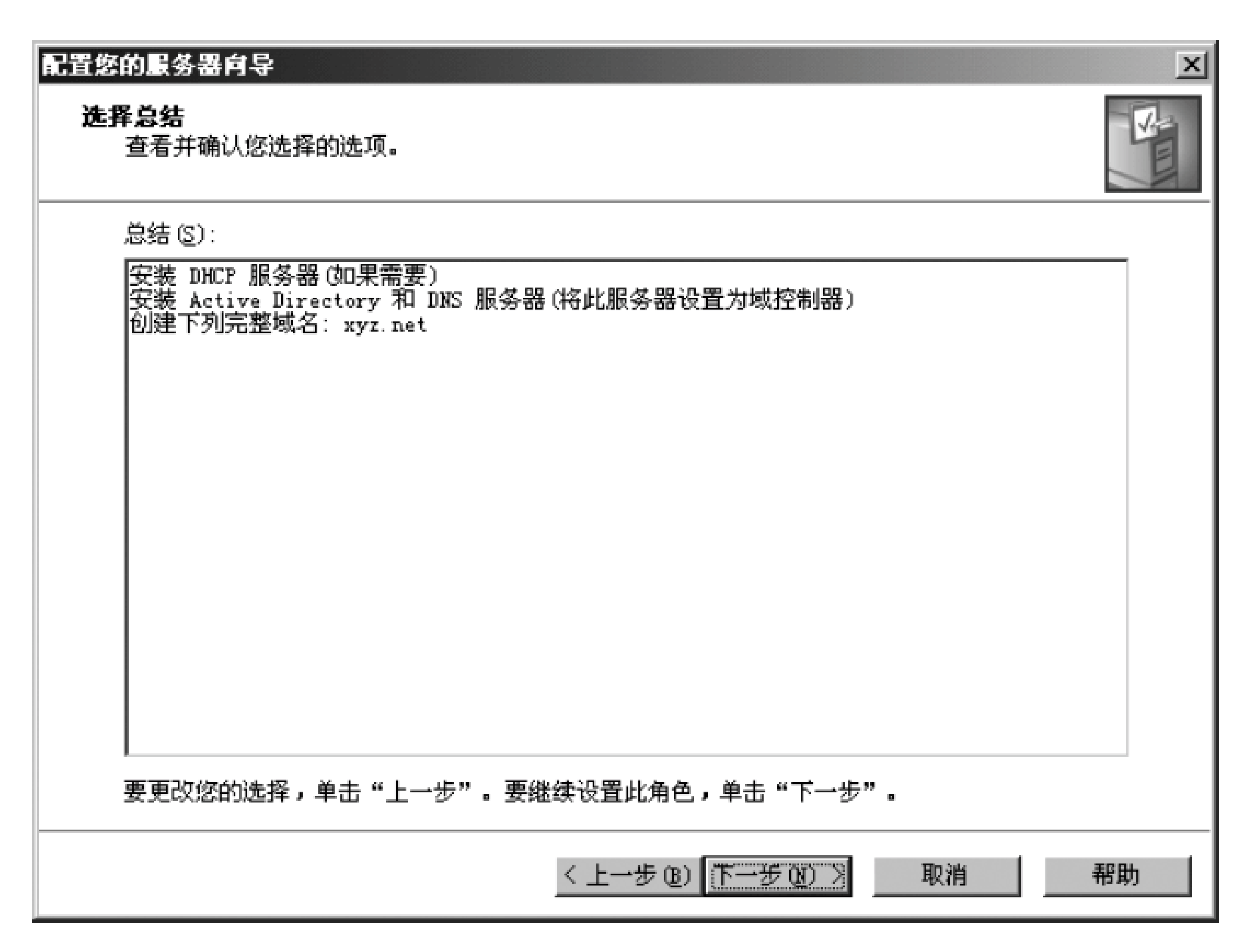


图 4-16　复查并确认选项



图 4-17　重新启动计算机

(10) 完成后，系统将自动重新启动，重新登录后还会继续执行后续的操作，服务器配置完成后，单击“下一步”按钮。

(11) 出现“此服务器现在已配置好”对话框时，单击“完成”按钮，即可完成域控制器的安装。

提示：通过典型配置方式，“目录服务还原模式”的管理员密码为空，如果要更改密码，可在进入“目录还原模式”后，通过按 Ctrl＋Alt＋Delete 组合键更改。

4.2.3　将计算机加入、脱离域

可以将 Windows XP Professional、Windows Server 2003、Windows 2000 Server / Professional、Windows NT Server/Workstation 等计算机加入域，以后用户就可以从这些成员计算机上，利用域用户账户登录到域并访问域的资源了。

要将计算机 pc01(已安装 Windows XP Professional)加入 xyz. net 域，操作步骤如下。

(1) 配置计算机 pc01 的“首选 DNS 服务器”为 192.168.10.1，即该域的第 1 台域控制器(同时也是 DNS 服务器)的 IP 地址。

(2) 在 pc01 上，右击“我的电脑”，选择“属性”，选择“计算机名”选项卡，单击“更改”

按钮。

(3) 出现如图 4-18 所示的对话框时,输入要加入的域名,单击"确定"按钮。

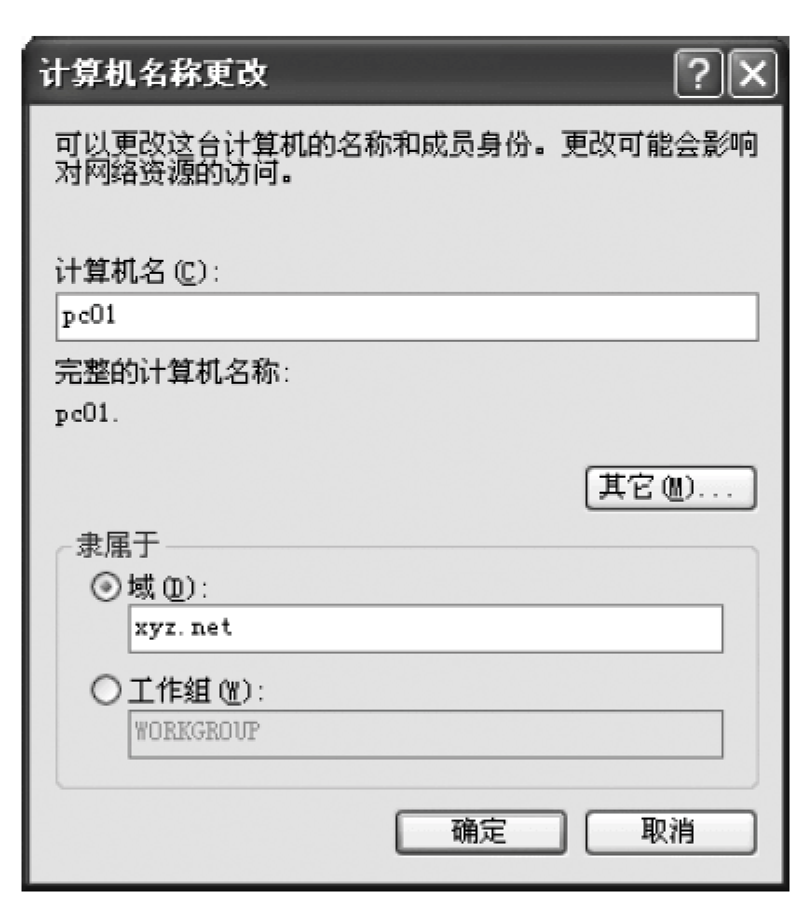


图 4-18 "计算机名称更改"对话框

(4) 如果出现图 4-19,表示当前计算机不能联系域控制器。原因有很多,一般要重点检查以下几个方面:域名是否输入正确;是否按步骤(1)所示为这台计算机配置了"首选 DNS 服务器";指定的 DNS 服务器的 IP 地址是否正确;DNS 服务器工作是否正常;网络连接是否正常等。在解决了这些问题后,再单击"确定"按钮,尝试重新加入域。

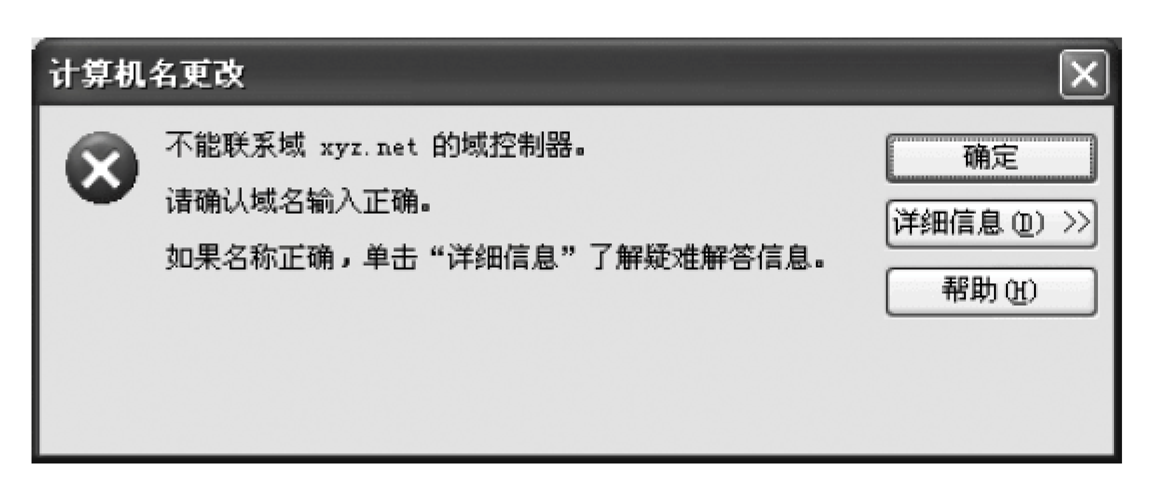


图 4-19 更改计算机名时不能联系域控制器

(5) 在如图 4-20 所示的对话框中,输入有权限将该计算机加入域的用户名与密码(例如 administrator),完成后,单击"确定"按钮。

提示: 任何一个域用户账户都可以将 10 台计算机加入域,但系统管理员不受此限制。

(6) 出现图 4-21,表示 pc01 已经成功加入域,单击"确定"按钮。

(7) 将计算机 pc01 成功加入域后,这台计算机的完整的计算机名称为 pc01.xyz.net,重新启动计算机即可生效。

将计算机(例如 pc01)加入域后,用户可以利用两种类型的账户登录。

① 域用户账户。在"登录到 Windows"对话框中,如图 4-22 所示,单击右下角的"选项"按钮后,输入管理员事先在域控制器上创建的域用户账户名(例如 user01)和密码,并选择登录到域(例如 XYZ)。登录成功后,该用户在访问域内的任何一台计算机时,都不





图 4-20　输入加入域的用户名和密码



图 4-21　提示成功加入域

需要再输入用户名和密码，这就体现了域的一个优点，即单次登录就可以访问域内的所有授权访问的资源。



图 4-22　“登录到 Windows”对话框

② 本地用户账户。在“登录到 Windows”对话框中，如图 4-23 所示，单击右下角的“选项”按钮，输入本地用户账户名 administrator 和对应的密码，并选择登录到“PC01(本机)”，成功登录以后，该用户就可以访问本地计算机内授权访问的资源，但无法访问域内其他计算机的上资源，除非在连接到其他计算机时再次输入有权限访问的用户名和密码。



图 4-23　登录到 Windows 本地计算机

将某台计算机脱离域的操作很简单,只需将如图 4-18 所示对话框中的隶属于"域"修改为"工作组",并且输入适当的工作组名称即可。工作组的名称可以自行设置,也可以输入网络中现有的工作组的名称。将计算机设置在同一个工作组后,用户在浏览网络上的计算机时,可以很容易找到同一个工作组内的计算机。

4.3 Active Directory 逻辑结构

Active Directory 的逻辑结构提供了在 Active Directory 中设计层次结构的方法,其逻辑组件包括域、组织单位、目录树和目录林、全局编录。

4.3.1 域

Active Directory 逻辑结构的核心是域。域是指由管理员定义的并由管理员管理的、共享通用目录数据库的计算机集合。域具有唯一的名称并且提供对用户账户和组账户的集中访问。

域提供了安全边界功能。使用安全边界的目的是为了确保域管理员只拥有对本域执行管理任务的必要权限,除非该管理员被明确授予其他域的管理权限。每个域都有自己的安全策略和与其他域关联的安全关系。

域也是复制单位。复制单位表示在特定域中所有的域控制器都能接收到该域中任何更改的信息,并能将更改的信息复制到该域中其他的域控制器上。

4.3.2 组织单位

组织单位(OU)用于在域中组织对象,例如用户账户、组、计算机、打印机和其他组织单位等对象。此外,还可以在组织单位上实施组策略。

1. 组织单位的层次结构

管理员可以结合网络需求和下列因素设计合理的组织单位层次结构,以便更加方便地组织、管理活动目录中的对象。

(1) 基于管理职责的网络管理模式。例如,某网络内可能会由一个管理员负责管理所有用户账户,而由另一个管理员负责管理所有计算机。这时,管理员就可以为用户对象和计算机对象分别创建一个组织单位。

(2) 基于部门或地理边界的组织结构。按照部门或地理位置划分组织结构。

(3) 上述两种层次结构的组合。

各个域的组织单位层次结构之间是互相独立的,每个域都可以实现自己的组织单位层次结构。

2. 管理组织单位

在 Active Directory 目录树的较高层次跟踪权限比跟踪对象或对象属性的权限更为简单,因此,最常用的委派管理控制方法是在组织单位或容器的级别上分配权限。在这个级别上分配权限,可以使管理员对该组织单位或容器内的所有对象进行委派管理控制。通过委派管理控制,无须网络中的最高管理员,受委派的管理员就可以执行指定的控制权限了。委派管理控制分散了管理操作,减少了管理的时间和成本,也减少了误操作的可能性。

4.3.3 域目录树、域目录林和双向信任传递

1. 域目录树

如果需要设置一个包含多个域的网络,则可以将网络设计为域目录树的结构,也就是说,这些域以树状的形式存在。图 4-24 显示了一个树状结构的域目录树,最上层的域名为 xyz. net,它是这个域目录树的根域,其下还有 2 个子域,分别是 bj. xyz. net 与 zz. xyz. net,在这些子域下面还可以设置更低一层的子域。

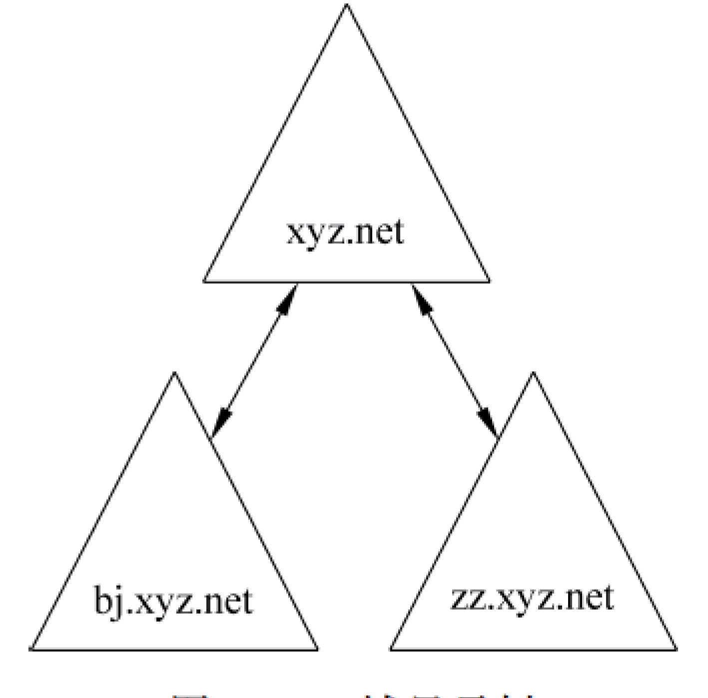


图 4-24 域目录树

目录树的名称空间是连续的,符合 DNS 域名空间的命名策略。子域的域名中包含着其父域的域名,例如,域 bj. xyz. net 中包含着上一层域(父域)的名称 xyz. net。

域目录树内的所有域共享一个活动目录,即在这个域目录树下只有一个活动目录。不过,这个活动目录内的数据分散地存储在各个域内,每个域中只存储该域的数据。Windows Server 2003 将存储在各个域中的对象总称为活动目录。

2. 域目录林

域目录林由一个或多个域目录树组成,每个域目录树都有自己唯一的名称空间,如图 4-25 所示,左侧域目录树内的每个域名的后缀都是 xyz. net,而右侧域目录树的每个域名的后缀都是 abc. net。

创建的第一个域目录树的根域,也是整个域目录林的根域,同时该域的域名也是域目录林的名称。例如,图 4-25 中的 xyz. net 是第一个域目录树的根域,它也是整个域目录林的根域,xyz. net 也是域目录林的名称。

虽然域目录林中的域目录树并不需要共享同一个连续的命名空间,但是共享相同的公共架构、Active Directory 配置的上下文和全局编录。如果一棵域目录树与其他任何域目录树都没有关联,那么它就形成一个仅含有一棵域目录树的域目录林。

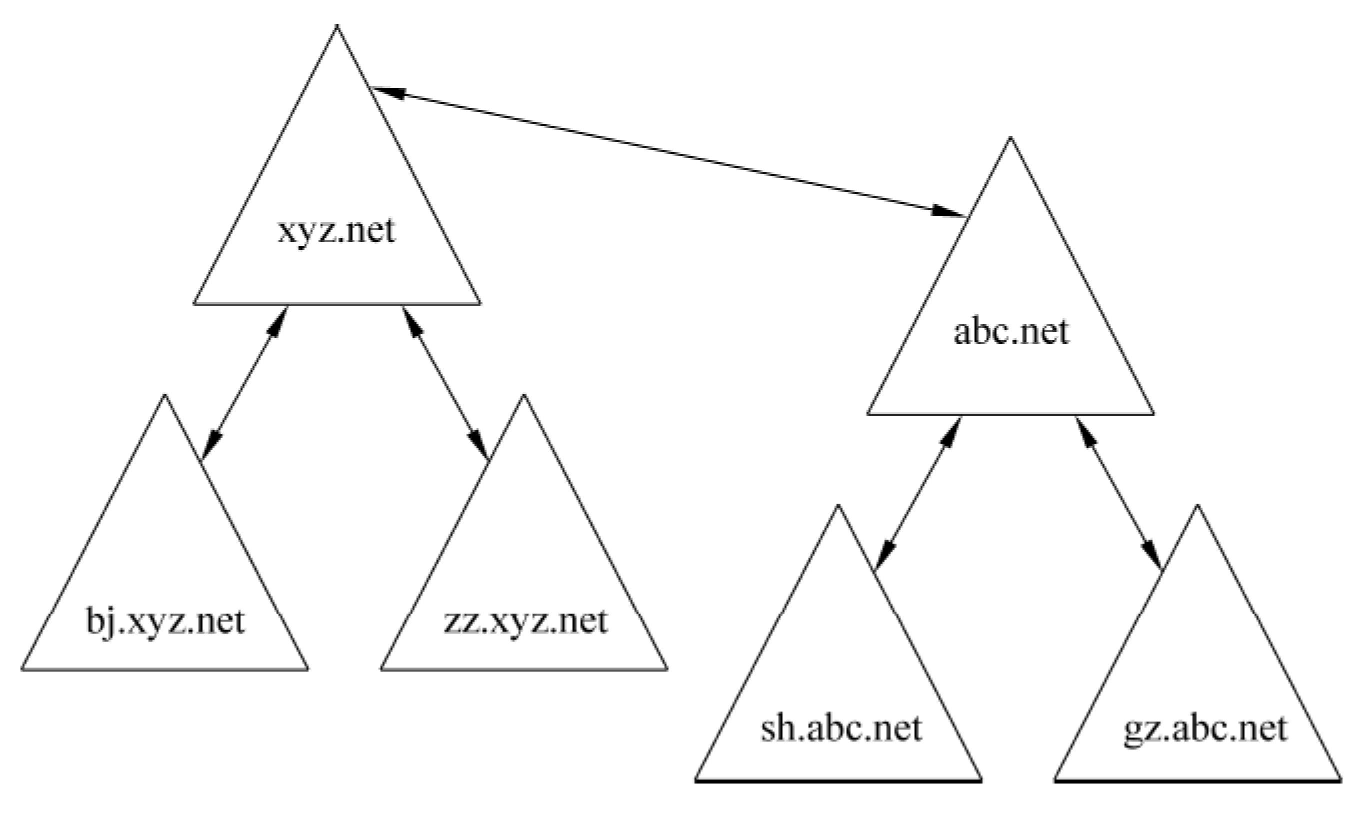


图 4-25 域目录林

3. 信任

两个域之间必须建立了信任关系，才可以访问对方域内的资源。任何一个域作为子域加入到域目录树后，这个子域会自动信任上一层的父域，同时父域也会自动信任这个子域，而且这些信任关系具备双向传递性。

在图 4-26 中，域 B 信任域 A(箭头由 B 指向 A)、域 A 又信任域 C，因此域 B 自动信任域 C；另外，域 C 信任域 A(箭头由 C 指向 A)、域 A 又信任域 B，因此域 C 自动信任域 B，因此，域 B 和域 C 之间也就自动建立了双向的信任关系，也称为隐含的信任关系，在图 4-26 中用虚线表示域 B 和域 C 之间隐含的信任关系。

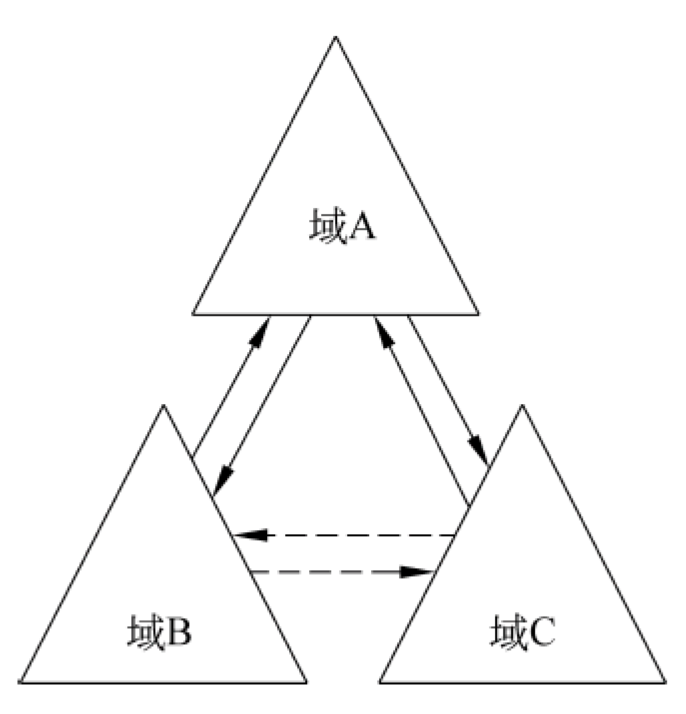


图 4-26 域之间的信任关系

当任何一个 Windows Server 2003 域加入到域目录树后，它会自动地双向信任这个目录树中的所有域，只要拥有适当的权限，这个新域内的用户就可以访问其他域内的资源；同理，其他域内的用户也可以访问这个新域内的资源。

创建域目录林时，每个域目录树的根域之间会自动建立双向的、可传递的信任关系。正是因为具备这种信任关系，所以，任何一个域内的用户都可以访问域目录林中任何一个域内的资源，也可以从任何一个域内的计算机上登录。

4.3.4 全局编录

前面讲过，虽然域目录树内的所有域共享一个活动目录，但是这个活动目录内的数据却是分散地存储在各个域内，而每个域只存储该域的数据。因此，为了让每个用户、应用程序能够快速地找到其他域中内的资源，Windows Server 2003 内就设置了“全局编录”。

全局编录是一个信息存储库,包含 Active Directory 中所有对象属性的一个子集。在默认状态下,将需经常查询的属性存储在全局编录中,如用户的姓名和登录名称。全局编录中也包含了用于确定对象在目录中位置的必要信息。全局编录还包括存储在全局编录中每个对象和属性的访问权限。如果用户在全局编录中搜索一个无权查看的对象,那么该对象将不会出现在返回的结果列表中。这保证了用户只能找到他们有权访问的对象。

全局编录让用户无须考虑对象在整个目录林中的位置,就可以很快地查找到所需对象。例如,当查询目录林中的所有打印机时,全局编录服务器在全局编录中执行查询并返回结果。如果没有全局编录服务器,那么就需要搜索目录林中的每个域才能完成该查询。全局编录还负责提供用户登录时,该用户所隶属的“通用组”数据。当用户利用用户主体名称(UPN)登录时,全局编录还负责提供该用户隶属于哪个域的信息。

全局编录服务器是一个用于处理查询全局编录请求的域控制器。在域目录林中创建的第一台域控制器就是默认的全局编录服务器。用户也可以通过配置额外的全局编录服务器来平衡登录认证和查询的流量。

4.4 Active Directory 物理结构

在 Active Directory 中,逻辑结构与物理结构是相互独立的、有区别的。用户使用逻辑结构组织网络资源,而使用物理结构配置和管理网络的流量。物理结构决定了在复制和登录时通信流量发生的时间和位置。域控制器和站点组成了 Active Directory 的物理结构。

4.4.1 域控制器

域控制器是一台运行 Windows Server 2003 并存储活动目录的计算机。域控制器通过活动目录提供目录服务,例如,它负责维护活动目录数据库、验证用户的账户与密码是否正确、将活动目录数据库复制到其他的域控制器。

一个域内可以有多台域控制器,多台域控制器可以提供足够的功能和容错功能,即使一台域控制器出现故障了,仍然能够由其他域控制器提供服务。另外,它还可以改善用户登录的效率,因为多台域控制器可以分担审核用户登录的负担。

1. SYSVOL 文件夹

SYSVOL 文件夹是一个共享的系统卷目录结构,存在于所有 Windows 2003 域控制器中。这个共享的系统卷存储了诸如登录、注销、启动和关闭脚本以及组策略信息之类的文件,这些文件会在域控制器间互相复制。这个共享的系统卷在不同的文件结构上会以不同的名称共享,在 Windows 2000 及其后续版本的客户端上为 SYSVOL,而在基于非 Windows 2000 的计算机上为 NETLOGON。SYSVOL 目录必须存放在基于 NTFS 文件系统的卷上。

2. Active Directory 复制

Active Directory 复制是 Active Directory 服务中最重要的功能之一。Active Directory 服务必须有多个域控制器，并且每个域控制器必须存储完全相同的 Active Directory 数据库副本，才能提供容错处理和负载平衡。管理员一旦更改了 Active Directory 中的信息，则发生更改的域控制器就会将更改的信息复制到本域中其他的域控制器中去。

Active Directory 数据库分为 3 个部分，称为命名上下文，分别如下。

(1) 域命名上下文。保存一个域中的所有对象和对象属性。

(2) 架构命名上下文。定义在 Active Directory 数据库中可创建的对象和属性。

(3) 配置命名上下文。保存目录林中与信任有关的信息。

域中的域控制器会将域命名上下文中的任何更改自动复制到其他域控制器。目录林中的域控制器会自动地将架构命名上下文和配置命名上下文中的任何更改复制到其他域控制器。复制保证了 Active Directory 中所有的信息对所有域控制器和网络中的客户端都可用。

Active Directory 大多使用多主机复制模式。在多主机复制模式下，每个 Windows 2003 域需要一个或多个域控制器。每个域控制器存储了一个可写的本地 Active Directory 数据库副本，并负责管理对该目录副本的修改和更新。如果用户或管理员更新了某个域控制器上的目录，则该更新信息将会复制到本域中所有其他的域控制器中去。然而在 Active Directory 同步更新前的一段时间内，各个域控制器可能会保存不同的信息。

3. 单主机操作

操作主机是指在 Active Directory 域或目录林中配备了一个或多个单主机操作角色的域控制器。它负责执行例如在目录林中添加域或删除域之类的操作，这类操作不允许在不同的域控制器上同时发生。单主机操作角色如下。

(1) 架构主机。用于控制目录林中所有对架构的更新。

(2) 域命名主机。用于控制在目录林中域的添加或删除。

(3) RID 主机。用于为本域中的每个域控制器分配相对标识(RID)序列。

(4) PDC 仿真主机。类似于 Windows NT 4.0 中的主域控制器(PDC)。

(5) 结构主机。用于在组成员身份发生变化时更新组到用户的关系，并将这些更新信息复制到域内的其他控制器。

同一个时间内，整个林中只能有一个架构主机、一个域命名主机，这两个角色默认由林根域内的第一台域控制器所扮演。而每个域中只能有一个 RID 主机、一个 PDC 仿真主机和一个结构主机，这 3 个角色默认由该域内的第一台域控制器所扮演。

4.4.2 站点

站点由一个或多个高速连接的 IP 子网组成。通过定义站点可以配置对活动目录复制和访问的拓扑路径，Windows Server 2003 可以使用最高效的链接和调度方法对复制和登录的流量进行控制。

一般来说，一个 LAN 内的各个子网之间的连接速度都够快且可靠性高，因此，可以将一个 LAN 规划为一个站点；而 WAN 内的各个 LAN 连接速度都不够快，因此 WAN 之间的各个 LAN 应该规划为不同的站点，如图 4-27 所示。

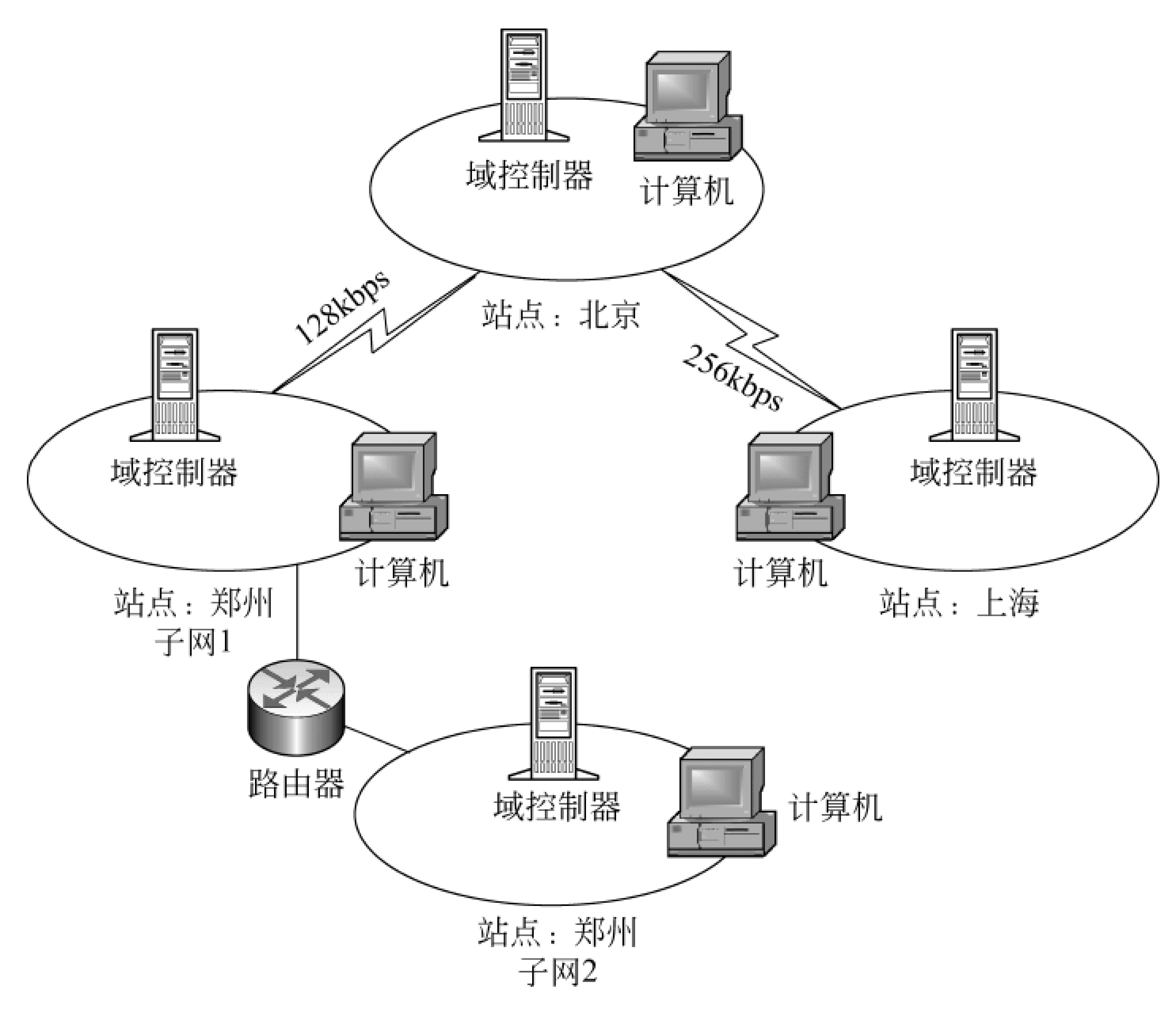


图 4-27 站点结构

为什么要建立站点呢？主要有以下两个目的。

（1）优化复制流量。

如果一个域的多台域控制器分布于不同的站点内，而这些站点之间是慢速连接在一起，在各个域控制器之间复制活动目录数据时，必须认真计划复制的时段，尽量避开高峰时间，复制的频率也不要太高，以免长时间占用站点之间的带宽，影响站点之间其他数据的传输效率。

同一个站点内的各个域控制器，由于是高速连接在一起，在复制活动目录数据时，可以有效地、快速地复制。活动目录会自动设置在同一站点内、隶属于同一个域的域控制器之间执行复制的频率，其默认的复制频率比站点之间的复制要高。

为了避免长时间占用站点之间的带宽，影响站点之间其他数据的传输效率，位于不同站点内的域控制器之间复制的数据会被压缩，而同一站点内的域控制器之间复制的数据

不会被压缩。

(2) 为用户连接到域控制器上进行登录和认证提供一个可靠的、高质量的网络连接。

Active Directory 的逻辑结构和物理结构相互独立。站点反映了网络的物理结构，域反映了网络的逻辑结构。在 Active Directory 中，每个站点可能会包含多个域，而每个域内的计算机也可能同时分别属于多个不同的站点。

4.5 在 Active Directory 中发布资源

可以在 Active Directory 中建立一个对象，使用户能够方便地查找需要经常访问的资源，例如共享文件夹、发布的打印机等。

4.5.1 发布资源介绍

发布资源就是指在 Active Directory 中建立对象，该对象直接包含需要的信息，或者提供对这种信息的引用。用户对象包含用户信息，如用户的电话号码和电子邮件地址。共享文件夹对象包含对网络中计算机的共享文件夹的引用。

只有在资源所包含的信息对用户非常有用，或者用户要求能够更方便、快捷地访问这些资源时，该资源才需要在 Active Directory 中发布，例如发布共享打印机、共享文件夹等。不需要发布 Active Directory 中已存在的资源，如用户账户、计算机账户。通常发布相对来说较少改变的信息，这样可以大大减少网络中的流量。

一旦在 Active Directory 中发布了资源，即使资源的物理位置发生变化，用户不需要任何操作就可以继续访问该资源。例如，如果管理员改变某个共享文件夹的位置，则已发布的共享文件夹的快捷方式将继续有效，因为已发布的共享文件夹仅仅是包含对共享文件夹本身的引用。

4.5.2 发布和管理打印机

域内的 Windows Server 2003、Windows XP Professional 或 Windows 2000 计算机上安装的共享打印机，默认会自动发布到 Active Directory 内，但早期版本的 Windows 系统(例如 Windows NT 4.0)上的打印机必须手动发布。

1. 控制 Windows Server 2003 上的打印机发布

如果要自行设置是否发布 Windows Server 2003 上的打印机，操作步骤为：单击“开始”→“打印机和传真”，右击打印机→“属性”，在图 4-28 中单击“共享”选项卡，选中或取消“列入目录”复选框。

也可以通过“Active Directory 用户和计算机”来查看被发布的打印机，在图 4-29 中，单击“查看”→“用户、组和计算机作为容器”命令，单击安装有打印机的计算机(例如 Server01)后，就可以看到被发布的打印机，如图 4-30 所示。

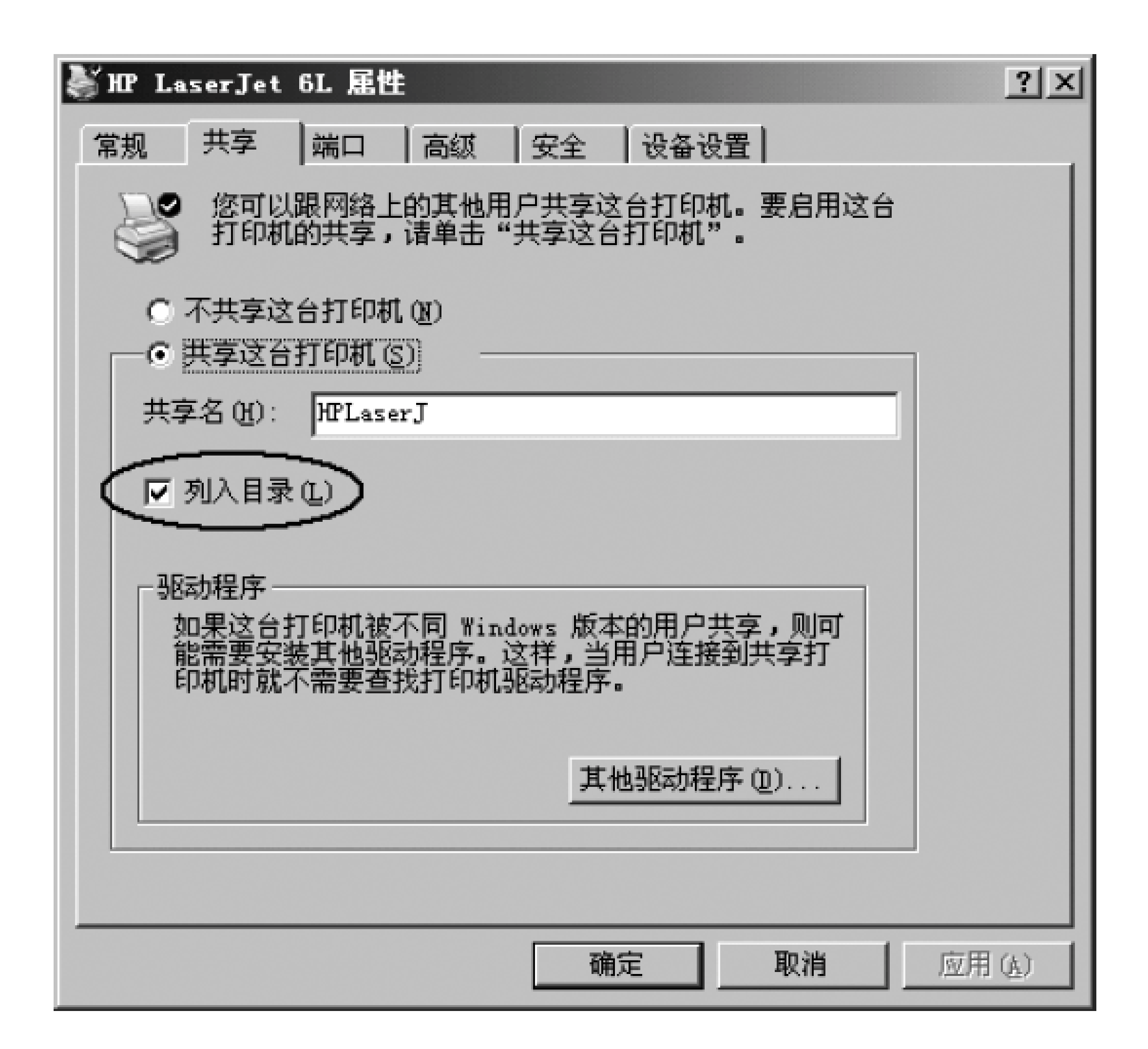


图 4-28　打印机属性

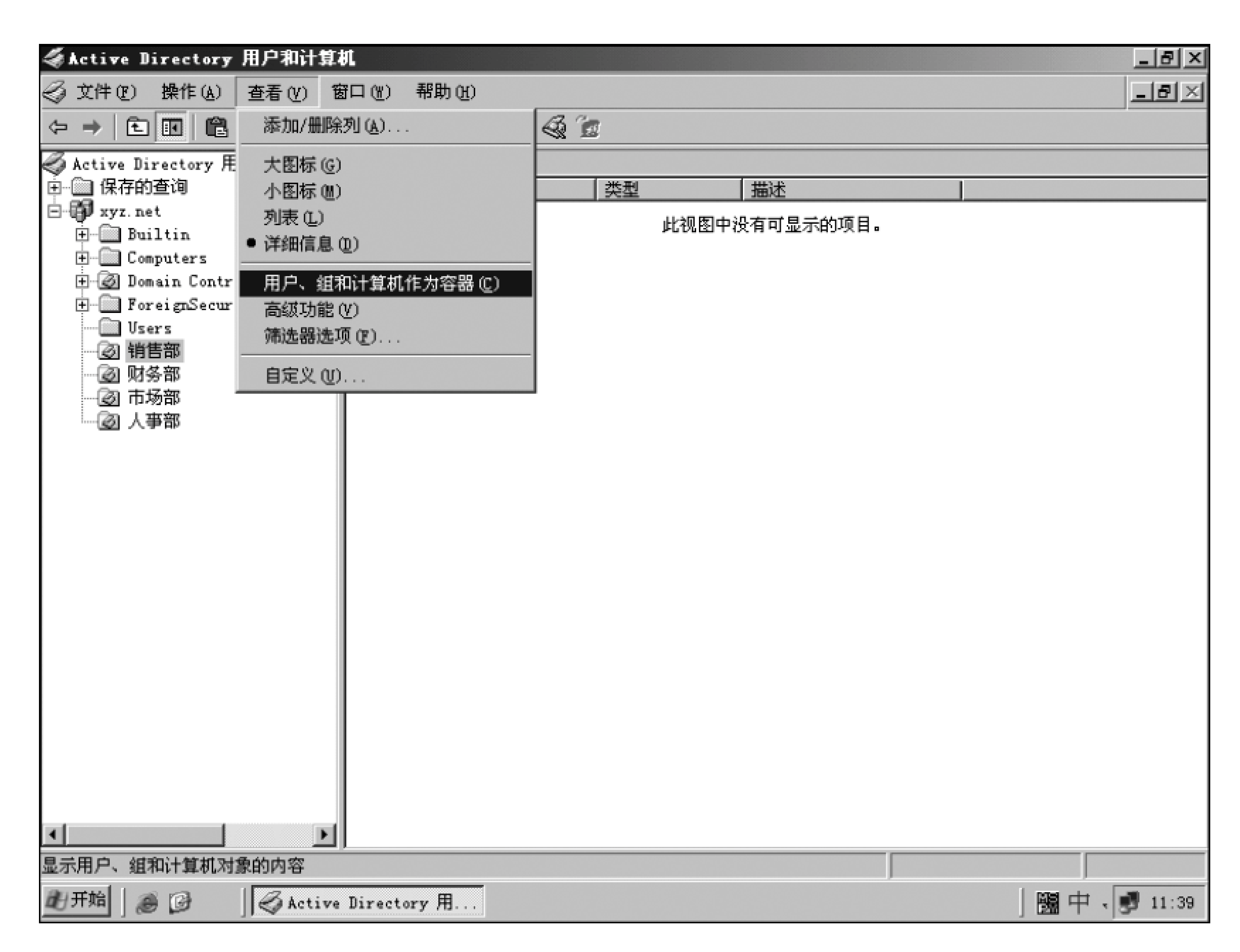


图 4-29　Active Directory 用户和计算机

提示：如果要取消 Windows Server 2003、Windows XP Professional 或 Windows 2000 计算机上的自动发布共享打印机的功能，可以通过组策略中的“计算机配置”→“管理模板”→“打印机”，自动在 Active Directory 上公布新的打印机。通过配置组策略，可以取消整个域或某个 OU 内的计算机自动发布共享打印机的功能。

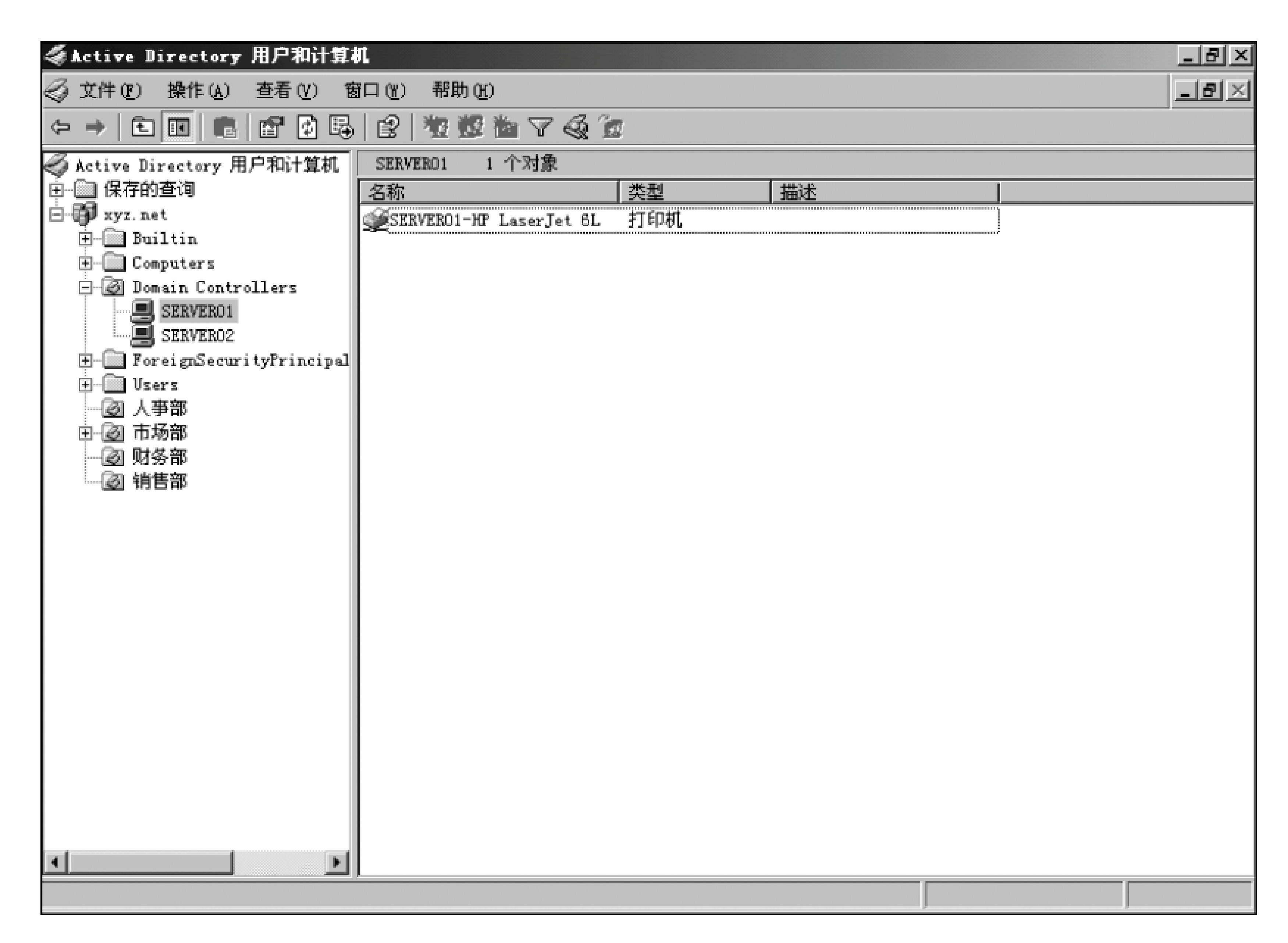


图 4-30 已被发布的打印机

2. 一般的打印机位置查找功能

如果为每一台打印机都设置“位置”属性的值,用户就可以通过“位置”属性来查找位于指定“位置”的打印机。在图 4-31 中,打印机位置被设置为“XYZ 公司 1 号楼”,则用户可以通过指定“位置”来查找位于“XYZ 公司 1 号楼”的打印机,如图 4-32 所示。



图 4-31 指定打印机的位置

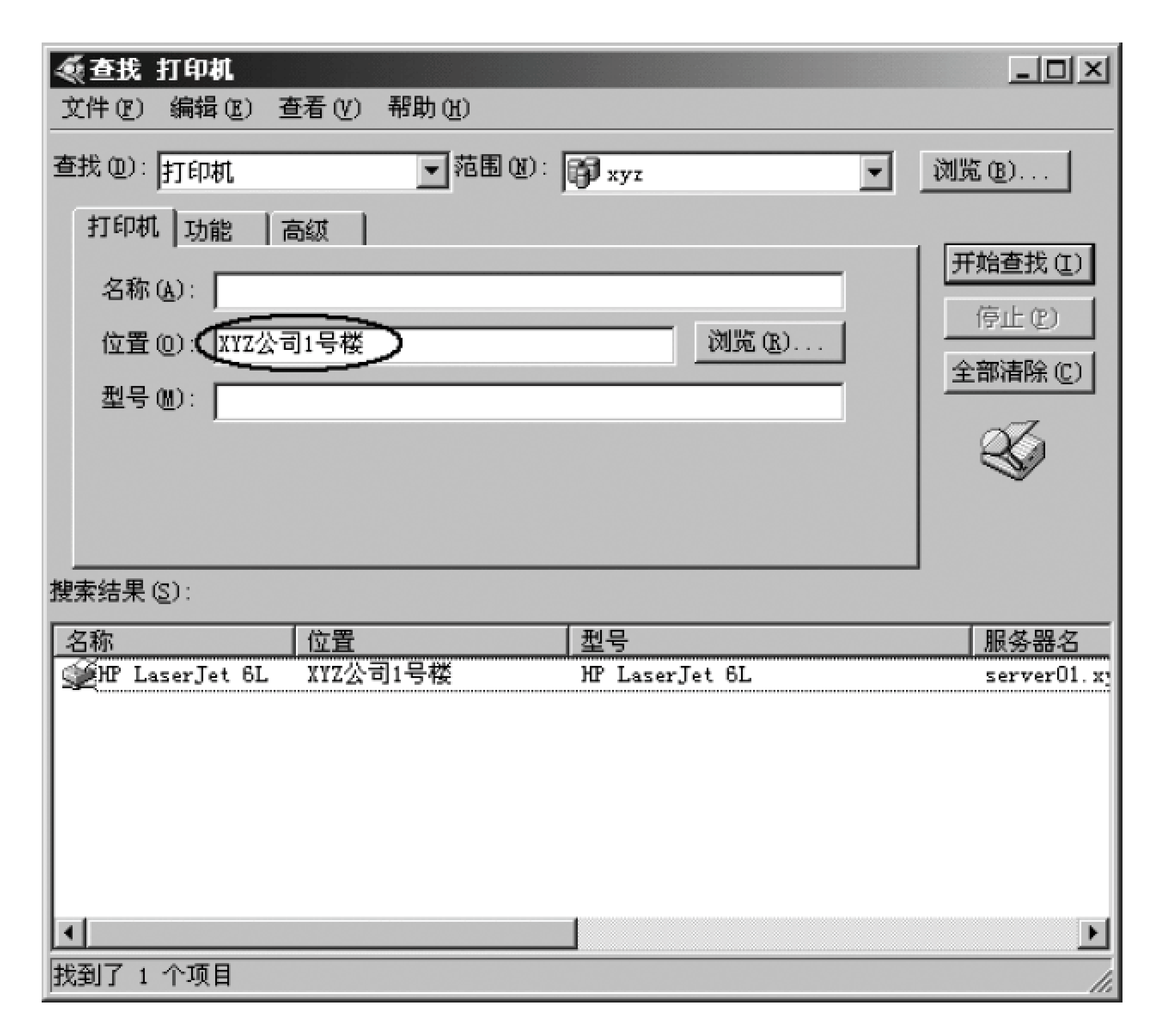


图 4-32　查找打印机

在设置打印机的“位置”属性时，建议采用类似“XYZ 公司 1 号楼”、“XYZ 公司 2 号楼”的格式，让用户在查找打印机时更为方便。

(1) 如果用户要查找位于“XYZ 公司 1 号楼”内的打印机时，只需要在“位置”处输入“XYZ 公司 1 号楼”即可。

(2) 如果用户要查找同时位于“XYZ 公司 1 号楼”和“XYZ 公司 2 号楼”的打印机时，用户在“位置”处输入 XYZ 后，系统就会为用户同时查找位于“XYZ 公司 1 号楼”和“XYZ 公司 2 号楼”内的打印机。

4.5.3　发布和管理共享文件夹

将共享文件夹发布到 Active Directory 后，域中的用户就可以通过 Active Directory 方便地查找、访问这个共享的资源。必须是 Domain Admins 或 Enterprise Admins 组内的用户，或是被赋予权限，才能发布共享文件夹。

要将计算机 Server01 内的共享文件夹“C:\公用文档”发布到“业务部”OU 内，操作步骤如下。

(1) 打开“资源管理器”，将“C:\公用文档”文件夹设为共享文件夹，假设共享名为“公用文档”。

(2) 打开“Active Directory 用户和计算机”，在如图 4-33 所示的对话框中，右击“人事部”，在弹出的快捷菜单中选择“新建”→“共享文件夹”命令。

(3) 在图 4-34 中，输入欲发布的共享文件夹的名称，并在“网络路径”中输入此共享文件夹的 UNC 路径，例如\\server01\公用文档。

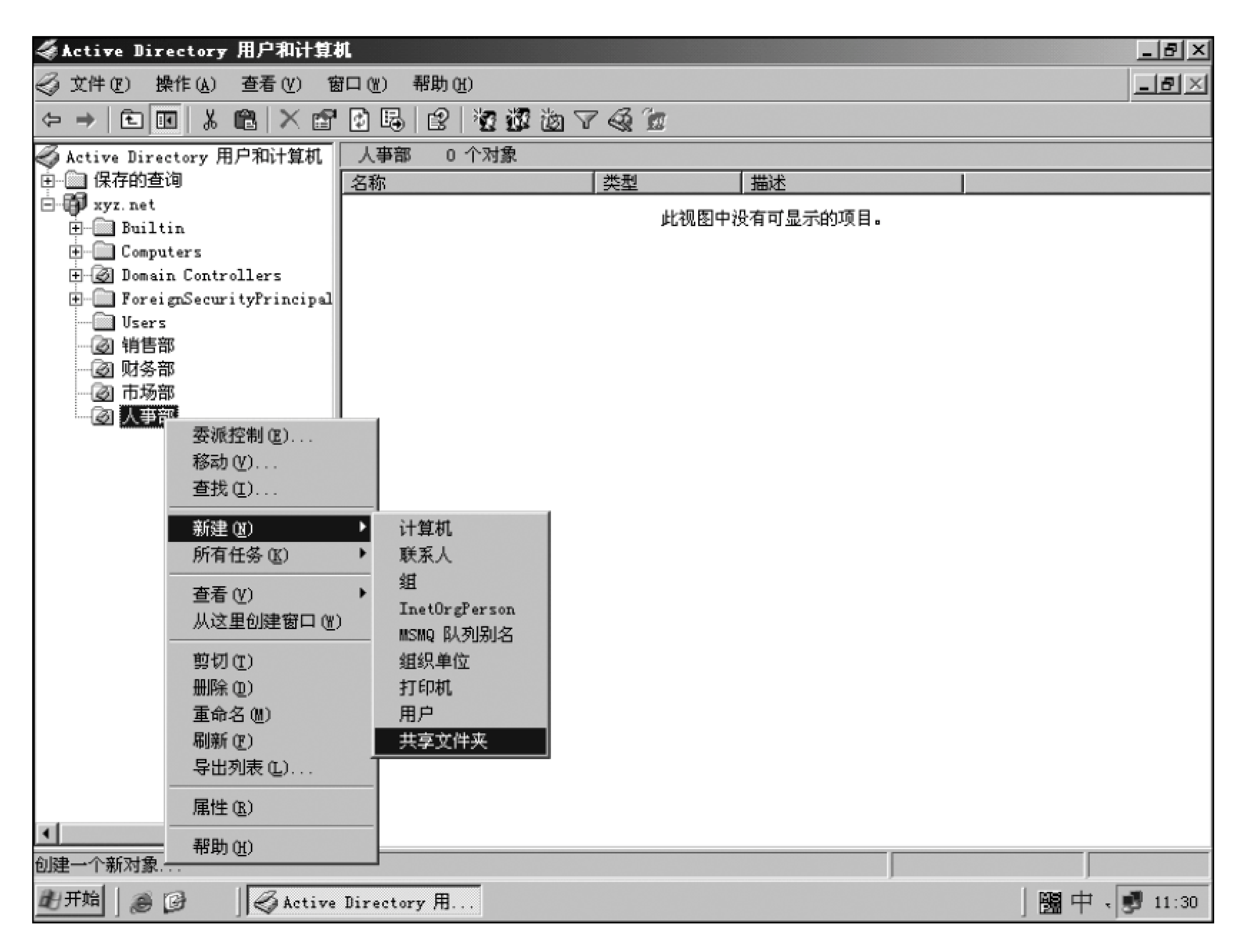


图 4-33　新建要发布的共享文件夹



图 4-34　指定要发布的共享文件夹的名称和路径

(4) 在图 4-35 中,右击“公用文档”,在弹出的快捷菜单中选择“属性”,在弹出的图中单击“关键字”按钮。

(5) 在图 4-36 中,添加关键字,单击“确定”按钮。

(6) 返回图 4-35,单击“确定”按钮。

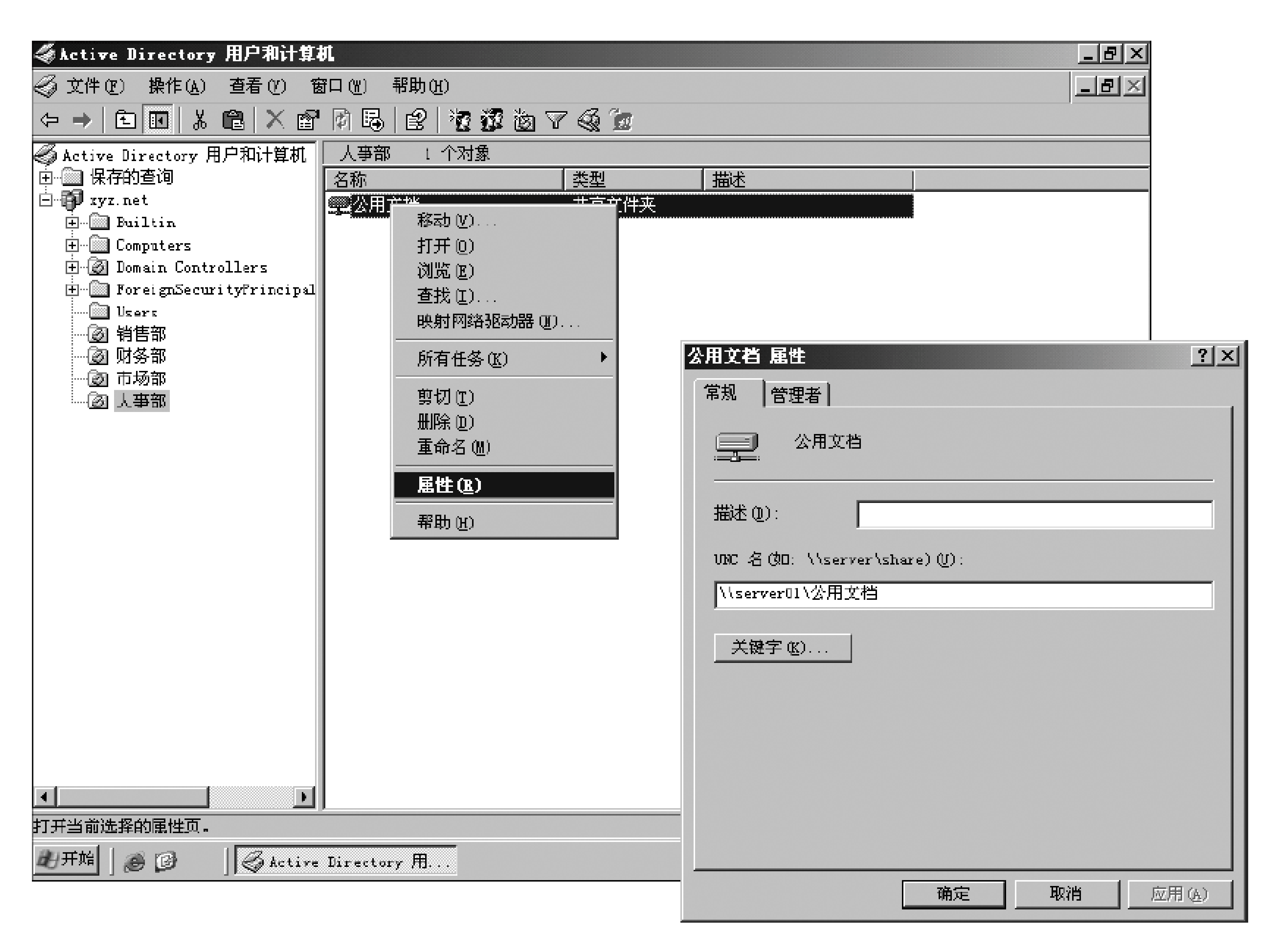


图 4-35　指定要发布的共享文件夹的关键字



图 4-36　添加关键字

4.5.4　查找 Active Directory 内的资源

域中的用户(包括系统管理员)可以通过多种方法来查找发布在 Active Directory 内的资源,利用“Active Directory 用户和计算机”、“网上邻居”是最常用的两种方法。

1. “Active Directory 用户和计算机”

“Active Directory 用户和计算机”管理单元的位置如下。

(1) 域控制器。单击“开始”→“管理工具”→“Active Directory 用户和计算机”。

(2) 成员服务器或 Windows XP Professional。必须运行 Windows 安装光盘的 I386

文件夹内的 ADMINPAK. MSI 来安装这个管理工具或者手工添加这个管理单元。

要利用“Active Directory 用户和计算机”管理单元来查找共享文件夹，可在如图 4-37 所示对话框中，右击域名称，在弹出的快捷菜单中选择“查找”，在弹出图中的“查找”下拉框中选择“共享文件夹”，并设置查找的条件(例如，输入共享文件夹的“关键字”)，单击“开始查找”按钮。

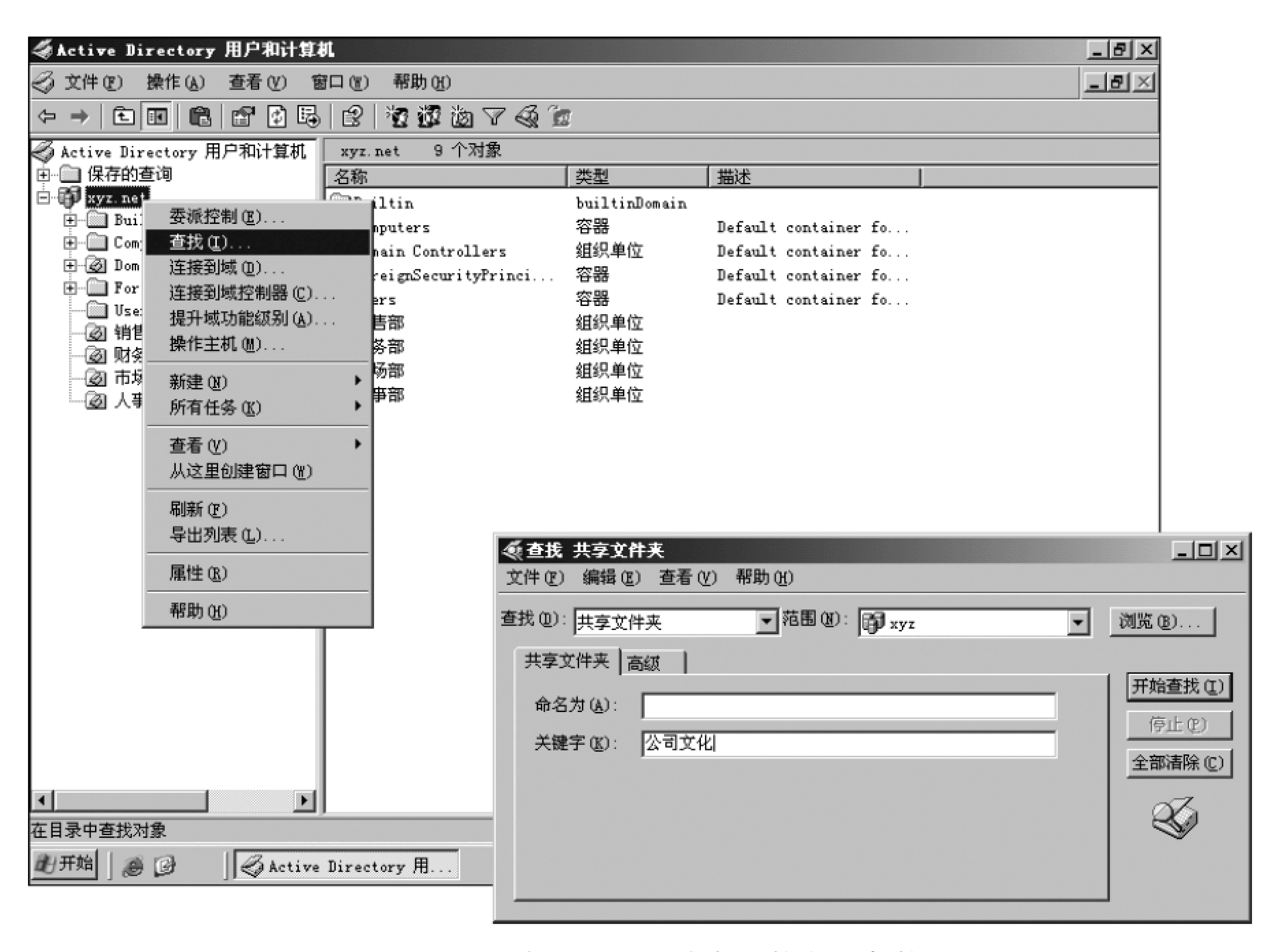


图 4-37 指定要查找的共享文件夹的条件

在图 4-38 中，通过右击查找到的共享文件夹来管理或访问此共享文件夹，或是直接双击来浏览里面的内容。

2. 网上邻居

(1) 通过自定义桌面项目，使桌面上显示“网上邻居”图标。操作步骤如下：右击“桌面”→“属性”→“桌面”选项卡→“自定义桌面”，在“常规”选项卡中选中“网上邻居”，单击“确定”按钮。

(2) 打开“网上邻居”，选择“工具”菜单→“文件夹选项”→“常规”选项卡，选择“在文件夹中显示常见任务”单选按钮，单击“确定”按钮。

(3) 在图 4-39 中，单击“搜索 Active Directory”，在“查找”下拉框中选择“共享文件夹”。



图 4-38 管理或访问共享文件夹

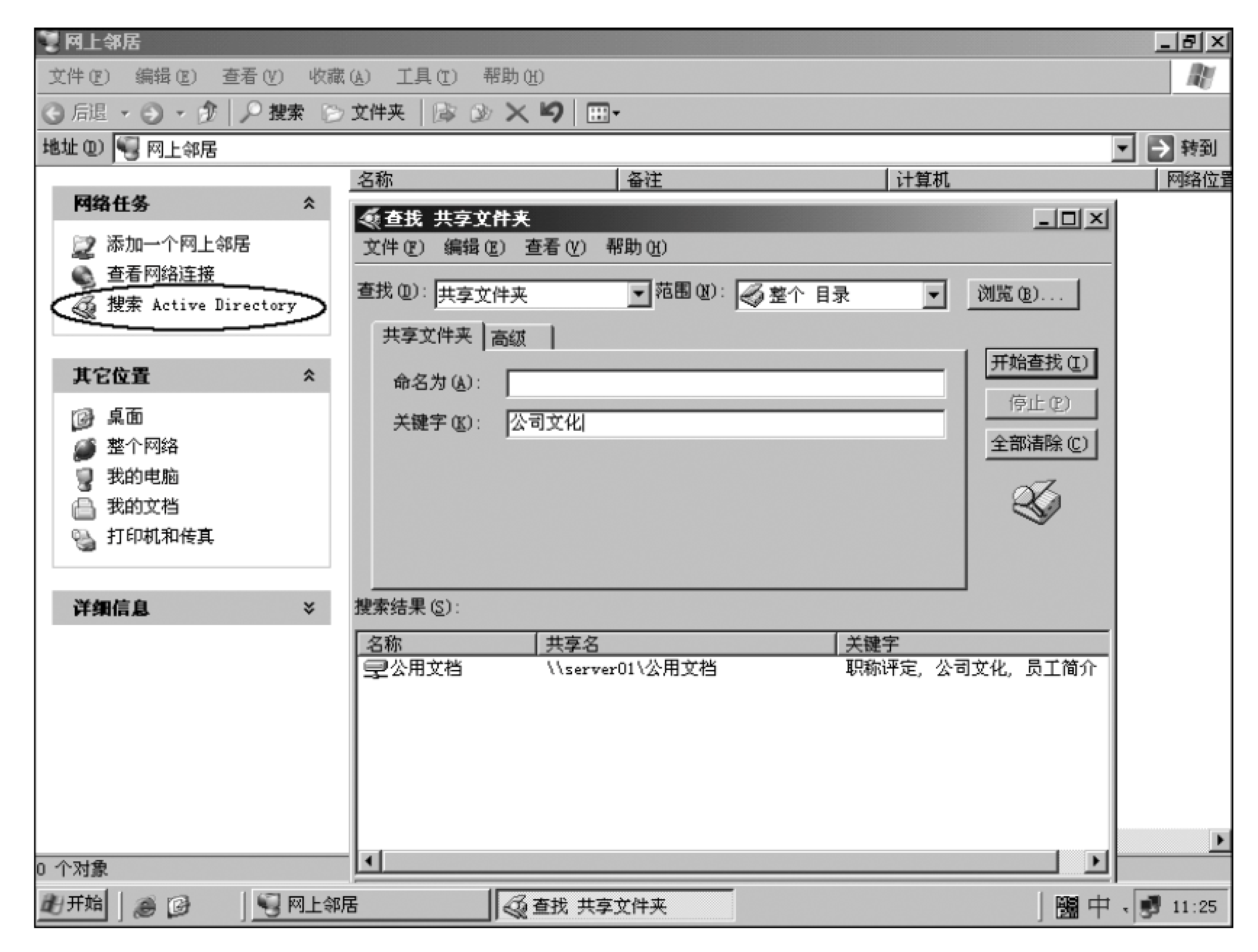


图 4-39 搜索 Active Directory 中已发布的共享文件夹

第 5 章　账 户 管 理

学习目标

学习完本章后，了解用户账户、组账户和计算机账户的功能。掌握本地用户账户和域用户账户的区别，并学会创建和管理本地用户账户和域用户账户。掌握用户配置文件、主文件夹的配置、使用方法。理解工作组中的组和域中的组的区别，特别是要理解域中的组的类型和作用域，并掌握使用域中的组的策略。

5.1　账户概述

网络中的每个用户都应该有一个用户账户，以便利用这个用户账户登录到域或本地计算机，从而访问域中的资源或者访问本地计算机上的资源。

组是用户账户的集合。管理员可以先将一组用户账户添加为某个组的成员，然后一次性为该组授予访问共享资源的权限，这时该组内的用户就会自动拥有授予组的权限，管理员不必为每个用户单独授予权限，这样就简化了对用户账户的管理。根据管理任务的需要，管理员还可以将计算机或者组添加为组的成员。

Active Directory 使用计算机账户来发布关于网络中的工作站、成员服务器和域控制器等计算机的一般信息（例如计算机的位置），并确保系统安全。当管理员要增加、删除计算机或者对目录进行修改时可能会用到计算机账户。

5.2　用户账户类型

Windows Server 2003 所支持的用户账户类型有以下两种。

（1）域用户账户。域用户账户存储在域控制器的 Active Directory 数据库内。用户可以利用域用户账户登录到域以访问网络资源。用户只需要一个用户账户和密码就能访问域中任何计算机上的资源。

当用户利用域用户账户登录时，这个账户数据会被送到域控制器，并由域控制器检查用户输入的账户名称和密码是否正确。

在某台域控制器上创建一个用户账户后，这个账户会被自动复制到同一个域内的其他所有域控制器内。当用户登录时，该域内的所有域控制器都可以检查用户输入的账户名称与密码是否正确。

（2）本地用户账户。本地用户账户是创建在非域控制器的“本地安全账户数据库”内，而不是域控制器的 Active Directory 数据库内。

用户可以利用本地用户账户登录到该账户所驻留的计算机，而且这个账户只能够访问这台计算机上的资源，而无法访问其他计算机上的资源。如果要访问其他计算机上的

资源，则必须输入访问其他计算机的账户名称和密码。

本地用户账户只存在于这台计算机内，它们既不复制到域控制器的活动目录，也不会被复制到其他计算机的“本地安全账户数据库”内。

当用户利用本地用户账户登录时，由这台计算机的“本地安全账户数据库”检查账户名称与密码是否正确。

除了本地用户账户和域用户账户外，Windows Server 2003 在安装完毕后还会自动创建一些内置的用户账户，常见的有两个。

（1）Administrator。Administrator 账户拥有管理域或本地计算机最高的权限。从安全的角度考虑，管理员可以更改该账户的名称，但是无法删除该账户。

（2）Guest。Guest 账户只有临时访问网络资源的最小权限，这个账户通常提供给临时需要登录计算机的用户使用。管理员可以更改该账户的名称，但是无法删除该账户。该账户默认是禁用的。

需要说明的是，本地的 Administrator 和 Guest 用户账户驻留在本地安全账户数据库内，域中的 Administrator 和 Guest 用户账户驻留在 Active Directory 数据库内。

5.3 用户账户和密码的命名约定

管理员在创建用户账户时，需要遵守网络上已经使用的约定和注意事项，这样可以更方便地创建、管理用户账户。

1. 账户的命名约定

账户的命名约定确定了如何在域中或本地计算机上命名、识别用户账户。使用一致的命名约定可以使管理员或用户更容易识别创建的用户账户名并方便以后的查找，账户的命名约定如下。

（1）账户名必须唯一，即域用户账户的用户登录名、全称在该用户账户所在的域里必须是唯一，本地用户账户的用户名在创建该本地用户账户的计算机上必须唯一。

（2）账户名不分大小写。

（3）账户名最多可以包含 20 个大、小写字符，输入时可以超过 20 个字符，但只识别前 20 个字符。

（4）可以使用字母、数字和特殊字符的组合来唯一地识别用户账户，但不能包含这些特殊字符："/ \ [ ] ：；| ＝ ，＋ * ？＜＞。

（5）账户名不能与组名相同。

2. 密码的命名约定

网络中的每个用户都要认识到设置复杂密码的重要性，树立使用复杂密码的意识，这有助于防止未经授权的个人登录到域或本地计算机。密码的命名约定如下。

（1）管理员账户的密码必须足够复杂，防止未经授权的访问。

（2）确定是由管理员还是由用户来管理密码，最好由用户来管理自己的密码。

(3) 使用难以被猜到的长密码,最多可以有 128 个字符,推荐使用至少 8 个字符的密码。

(4) 密码要使用大、小写字母、数字和特殊字符的组合,如果密码内包含英文字母,要区分大小写,例如 abc 与 ABC 是不同的密码。

(5) 避免使用有明显关联的密码,例如电话号码、名字、生日等。

(6) 管理员最好通过配置组策略中的密码策略来强制用户使用复杂的密码。

5.4 本地用户账户

只在 Windows 2003/2000/NT 独立服务器或成员服务器、Windows XP/2000 Professional、Windows XP Home Edition、Windows NT Workstation 等未加入域的计算机内创建本地用户账户,本地用户账户驻留在这些计算机的本地安全账户数据库内。

利用本地用户账户只能登录到此账户所在的计算机,并且只能访问这台计算机内的资源,无法访问网络上其他计算机内的资源。

1. 创建本地用户账户

在 Windows Server 2003 计算机中,创建本地用户账户的步骤为:单击“开始”,右击“我的电脑”→“管理”,或者单击“开始”→“管理工具”→“计算机管理”,展开“计算机管理”→“系统工具”→“本地用户和组”→“用户”,右击“用户”→“新用户”,如图 5-1 所示。

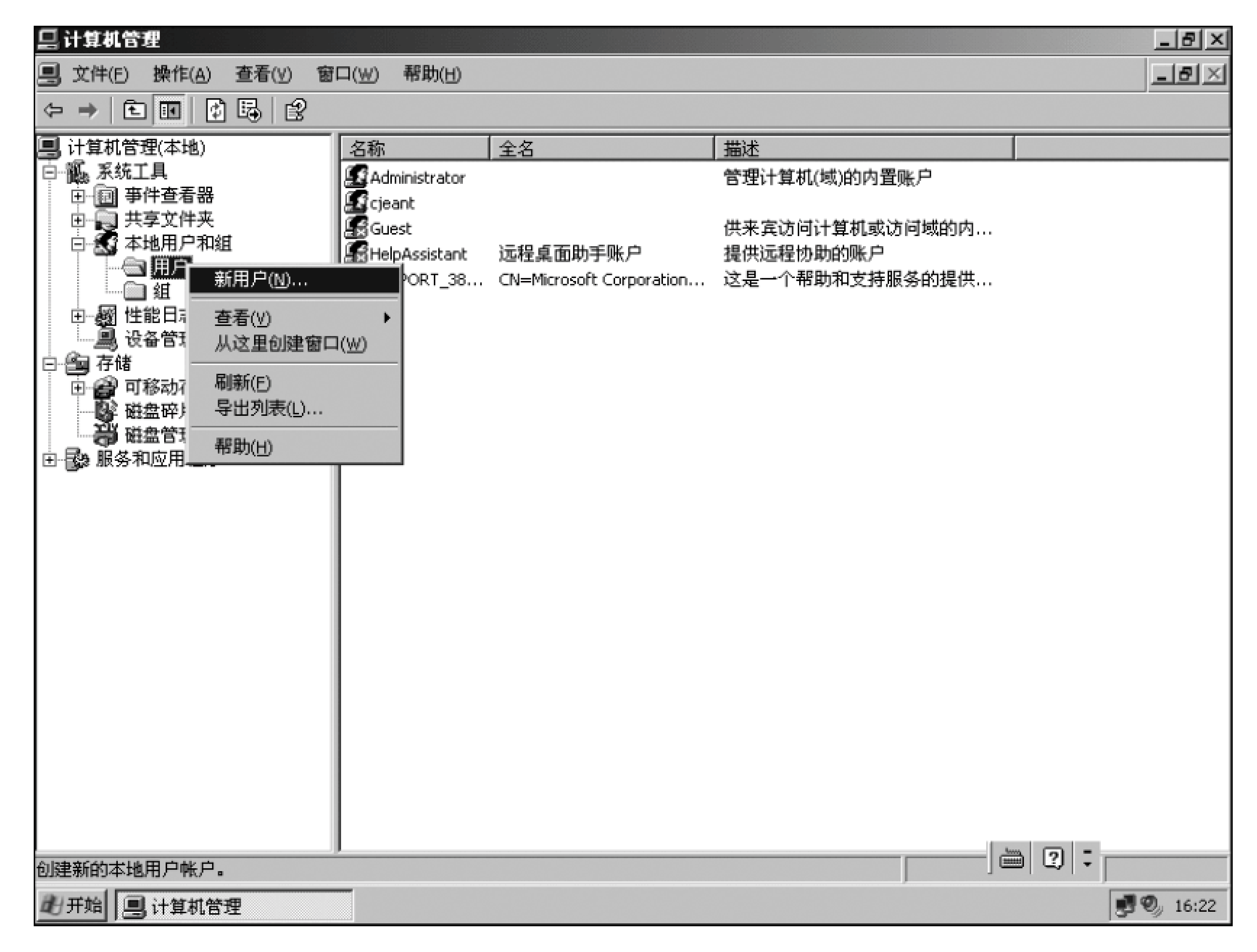


图 5-1 创建本地用户账户

在图 5-2 中,输入并设置账户的相关信息后,单击“创建”按钮。创建好本地用户账户

后，就可以利用此账户登录到本地计算机了。

图 5-2　指定新用户的信息

关于更多的账户信息选项，如表 5-1 所示。

表 5-1　账户信息选项

选　　项	描　　述
用户名	登录计算机时要使用的账户登录名称
全名	用户的完整名称
描述	用来描述用户的说明性文字
密码、确认密码	输入用户账户的密码，并再次输入密码以确认两次输入的密码是否一致
用户下次登录时须更改密码	用户下次登录时，系统显示一个强制用户更改密码的对话框。管理员事先已经为用户创建了账户并预置了密码，此项可以确保用户使用最新的密码
用户不能更改密码	防止用户更改密码。若是多人使用一个账户，可避免密码被其中一个用户修改
密码永不过期	选择选项后，系统不会要求该用户更改密码，即使在“账户策略”的“密码最长有效期”中设置所有用户必须定期更改密码，也不会要求这个用户更改密码（系统默认是 42 天更改密码）
账户已禁用	防止用户利用此账户登录。可以利用此项设置某个长期出差的员工的账户、临时不用的用户账户、尚没启用的用户账户的状态为禁用

提示：

（1）用户无法在域控制器内创建本地用户账户。

（2）默认情况下，使用空白密码的用户只能够登录到本地计算机，无法通过网络登录到其他计算机。

2．修改本地用户账户信息

如果要修改本地用户账户的登录名称，只要右击该账户，选择“重命名”即可。如果要更改本地用户账户的密码，可以在登录后按 Ctrl＋Alt＋Del 组合键，如图 5-3 所示，输入

正确的旧密码后，然后再设置新密码。若要修改本地用户账户的其他信息，只要右击该账户，选择“属性”即可。



图 5-3　修改本地用户账户密码

5.5　域用户账户

利用“Active Directory 用户和计算机”管理单元，管理员可以在任何一个容器或者组织单位(OU)内创建域用户账户。

5.5.1　创建域用户账户

先创建一个名称为“市场部”的组织单位，然后在此组织单位内创建一个域用户账户 cuijiantao，操作步骤如下。

(1) 打开“Active Directory 用户和计算机”→右击域名(例如 xyz.net)→“新建”→“组织单位”→输入组织单位的名称(例如市场部)。

(2) 在图 5-4 中，右击“市场部”，在弹出的快捷菜单中选择“新建”→“用户”命令。

(3) 在图 5-5 中，输入相关的账户信息后，单击“下一步”按钮。

域用户账户的信息如表 5-2 所示。

表 5-2　域用户账户的信息

选　　项	描　　述
姓、名	在这两个文本框中至少输入一项数据
姓名	用户的完整姓名，默认是姓与名的组合
用户登录名	用户登录域时所使用的名称，也就是用户主体名称(UPN)。在 Windows Server 2003、Windows XP Professional、Windows 2000 等计算机登录域时使用这个名称。在整个域目录林内，这个名称必须是唯一的。
用户登录名(Windows 2000 以前版本)	这个名称是供 Windows 2000 以前版本的客户端使用的，例如 Windows NT、Windows 98 等，用户在这些计算机上登录时，必须使用这个名称。在同一个域内，这个名称必须是唯一的

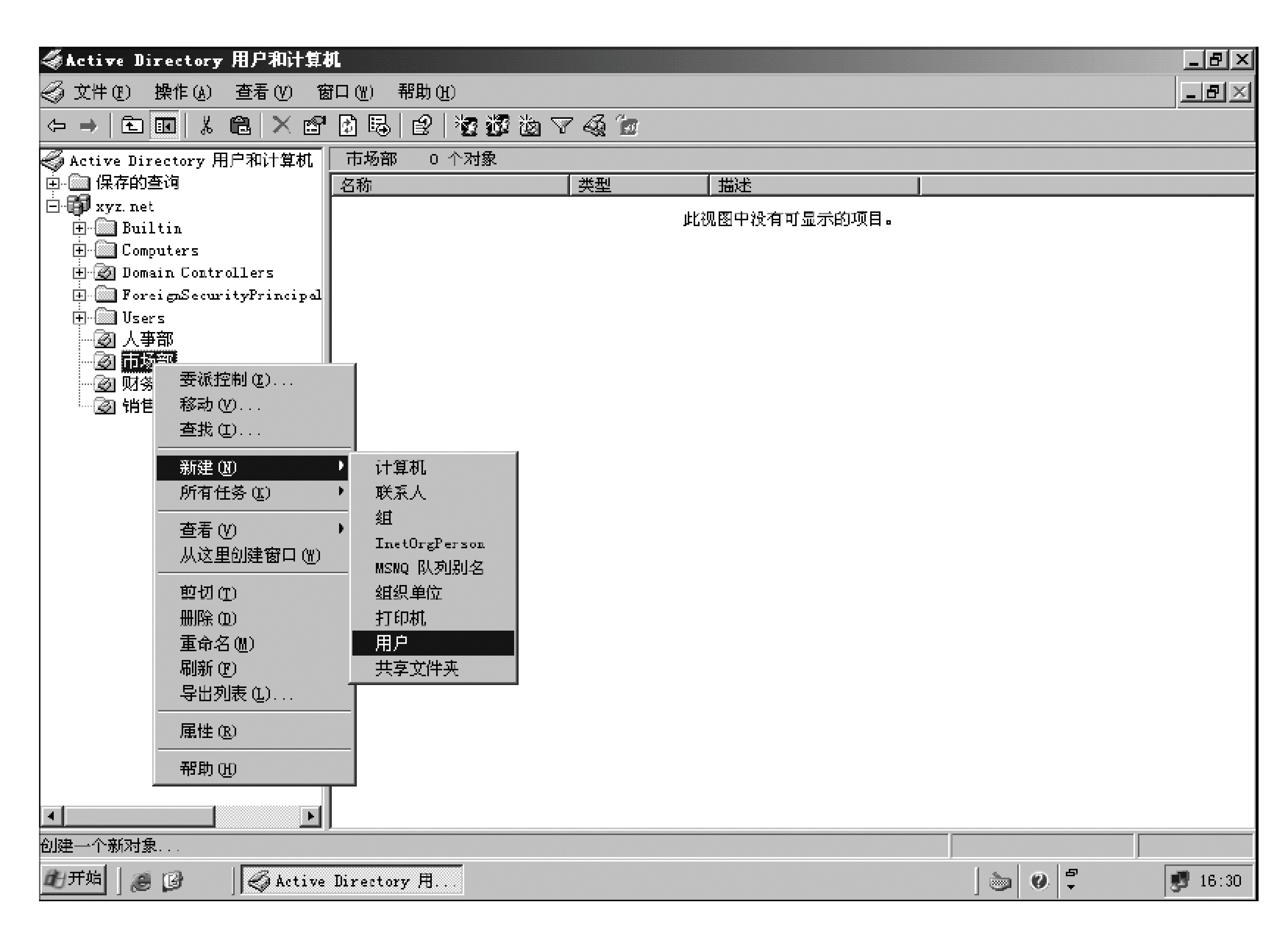


图 5-4　新建域用户账户



图 5-5　指定域用户账户信息

(4) 在图 5-6 中，设置好相应的选项后，单击“下一步”按钮即可完成域用户账户的创建。

提示： 在 Windows Server 2003 域中，默认情况下所有用户账户的密码必须至少 7 个字符，并且不可以包含用户账户名称的全部或部分文字，至少要包含 A～Z、a～z、0～9、特殊字符(例如@、!、￥、#、%等)4 组字符中的 3 组。可以通过“域安全策略”中的“密码策略”设置密码的复杂性。

创建域用户账户后，就可以从隶属于域的计算机上(例如 Windows XP Professional)利用这个域用户账户登录了，如图 5-7 所示。在“登录到 Windows”对话框中输入用户名、密码，选择登录到域(例如 ABC)。



图 5-6 设置域用户账户的选项



图 5-7 使用域用户账户登录

如果是在 Windows Server 2003、Windows XP Professional、Windows 2000 上登录到域,还可以输入用户主体名称(UPN)和密码登录,如图 5-8 所示。

5.5.2 设置域用户账户的属性

网络中的用户可以通过域用户账户的地址、电话、电子邮件等属性信息查找活动目录内的用户。

打开"Active Directory 用户和计算机"管理单元,右击用户账户,在账户"属性"对话框中,可以设置域账户的属性。域用户账户的属性有很多,下面仅介绍主要属性。



图 5-8　使用用户主体名称登录

1. 用户个人信息的设置

用户个人信息在账户属性对话框中的“常规”、“地址”、“电话”、“单位”等选项卡内设置，在图 5-9 中用圆圈标记。

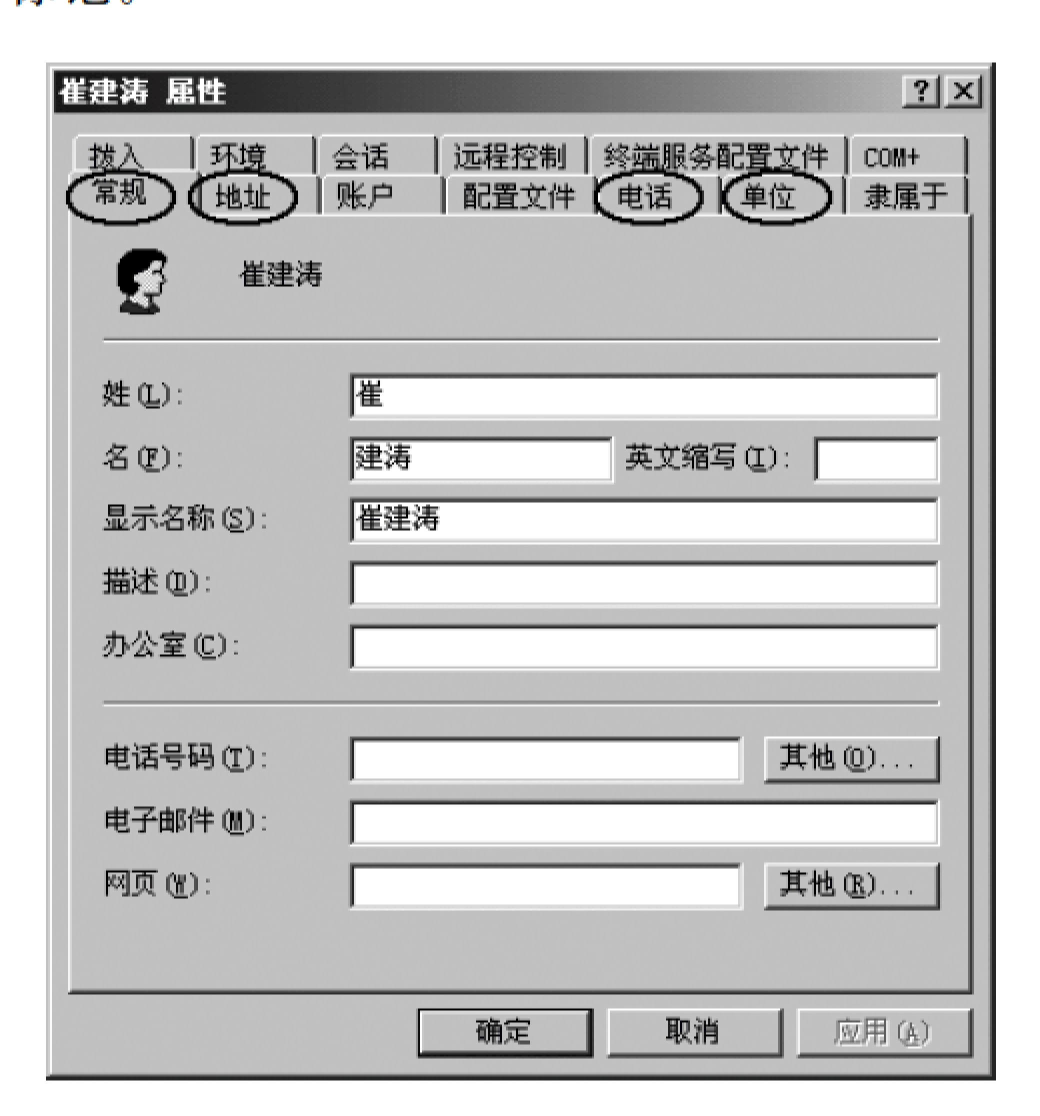


图 5-9　个人信息

2. 账户信息的设置

账户信息在“账户属性”对话框的“账户”选项卡内设置，如图 5-10 所示。其中大部分信息与本地用户账户相同。在此仅介绍“账户过期”属性，它用来设置账户过期的日期，默认为账户永不过期。要设置账户过期的截止日期，单击“账户”选项卡→“账户过期”，单击“在这之后”，选择一个截止日期，单击“确定”按钮。



图 5-10 “账户”选项卡

3. 登录时间的设置

登录时间用来设置用户登录到域的时间。默认任何时间都可以登录到域。要更改登录时间设置,在图 5-10 中单击“登录时间”按钮,将出现图 5-11。

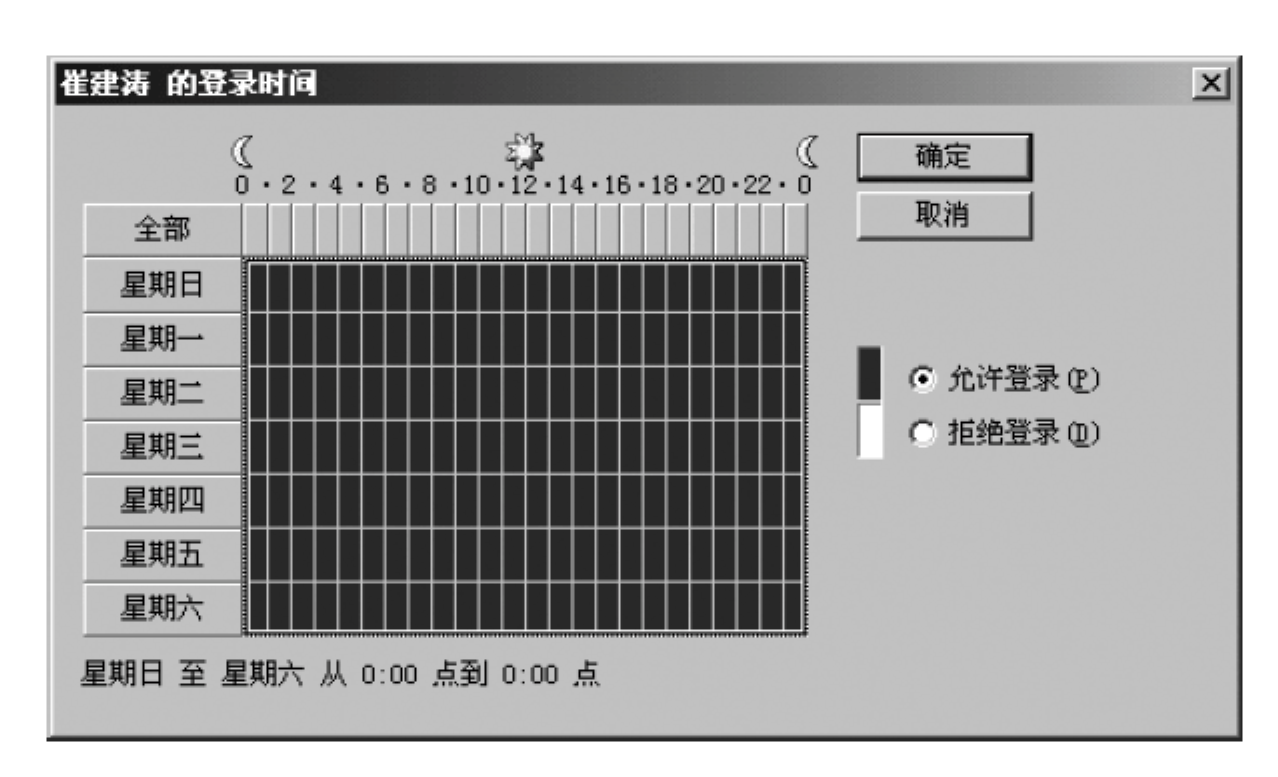


图 5-11 登录时间

在图 5-11 中,横轴每一方块代表一小时,纵轴每一方块代表一天,蓝色方块表示允许用户登录,白色方块表示拒绝用户登录,默认是用户可以在任何时间登录域。

要设置用户登录时间,操作步骤如下。

(1) 在图 5-11 中,选择时间段,方法如表 5-3 所示。

(2) 如果单击“允许登录”单选按钮,则表示在步骤(1)内所选的时间允许用户登录;如果单击“拒绝登录”单选按钮,则表示在该时段内不允许用户登录。

(3) 完成后,单击“确定”按钮即可。

表 5-3　选择时间段的方法

选择时间段	方　　法	选择时间段	方　　法
一个小时	单击代表该小时的方块	某一天的某小时	单击该小时最上端的方块
数小时	从开始方块拖曳到结束方块	整周	单击左上角的“全部”
一整天	单击左侧的“星期×”方块		

4. 设置用户只能在某些计算机登录

默认情况下，用户可以在域内的任何一台计算机登录到域。根据管理的需要，可以设置用户只能在某些计算机登录到域。

要设置用户可以在哪些计算机登录，操作步骤为：单击图 5-10 中的“登录到”按钮，然后在图 5-12 中，输入用户可以登录的计算机名称（例如 PC01），这个名称必须是 NetBIOS 计算机名称，然后单击“添加”按钮，再单击“确定”按钮即可。



图 5-12　登录的计算机

5. 更改域用户账户

要更改域用户账户的信息，操作步骤为：右击要更改的用户账户，然后通过右键菜单中的重命名、删除、禁用账户、启用账户、重设密码与解除被锁定的账户等进行设置，如图 5-13 所示。

（1）禁用账户、启用账户。例如，某个员工暂时出差，不需要使用公司的计算机，则管理员可以先将该员工的账户禁用，等该员工回公司上班后，再启用账户。禁用账户后，则该账户的图标上会出现一个红色的×号。

（2）重命名。重命名账户后，该用户账户原来所拥有的权限、权利与组关系都不会受影响。例如，当某个员工离职时，管理员可以先将该员工的用户账户禁用，等到新进的员工接替他的工作时，再将此账户重命名为新员工的名称，并重新设置密码等信息。

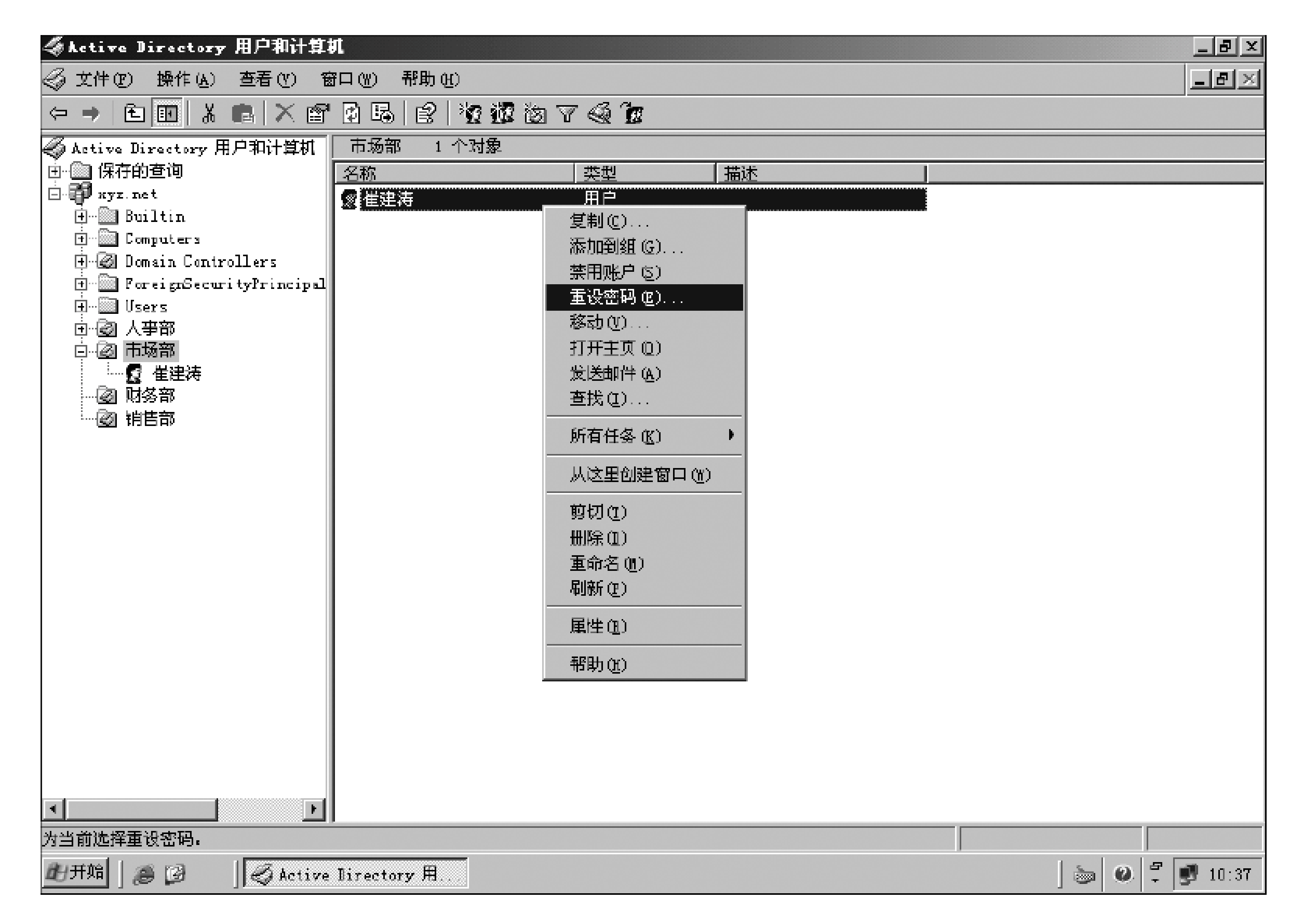


图 5-13 更改域用户账户

(3) 删除账户。如果某个员工辞职了，并且这个账户以后再也用不到时，则可以删除该账户。

(4) 重设密码。当用户忘记密码或密码过期时，系统管理员可以为用户重新设置一个密码。

(5) 解除被锁定的账户。管理员可以在组策略中设置"账户锁定策略"，定义用户在若干次无效登录(输入用户名、密码错误)之后将账户锁定。在用户账户被锁定以后，管理员可以解除被锁定的账户：打开"Active Directory 用户和计算机"，右击该用户账户→"属性"→"账户"选项卡，取消"账户已锁定"复选框，如图 5-14 所示。

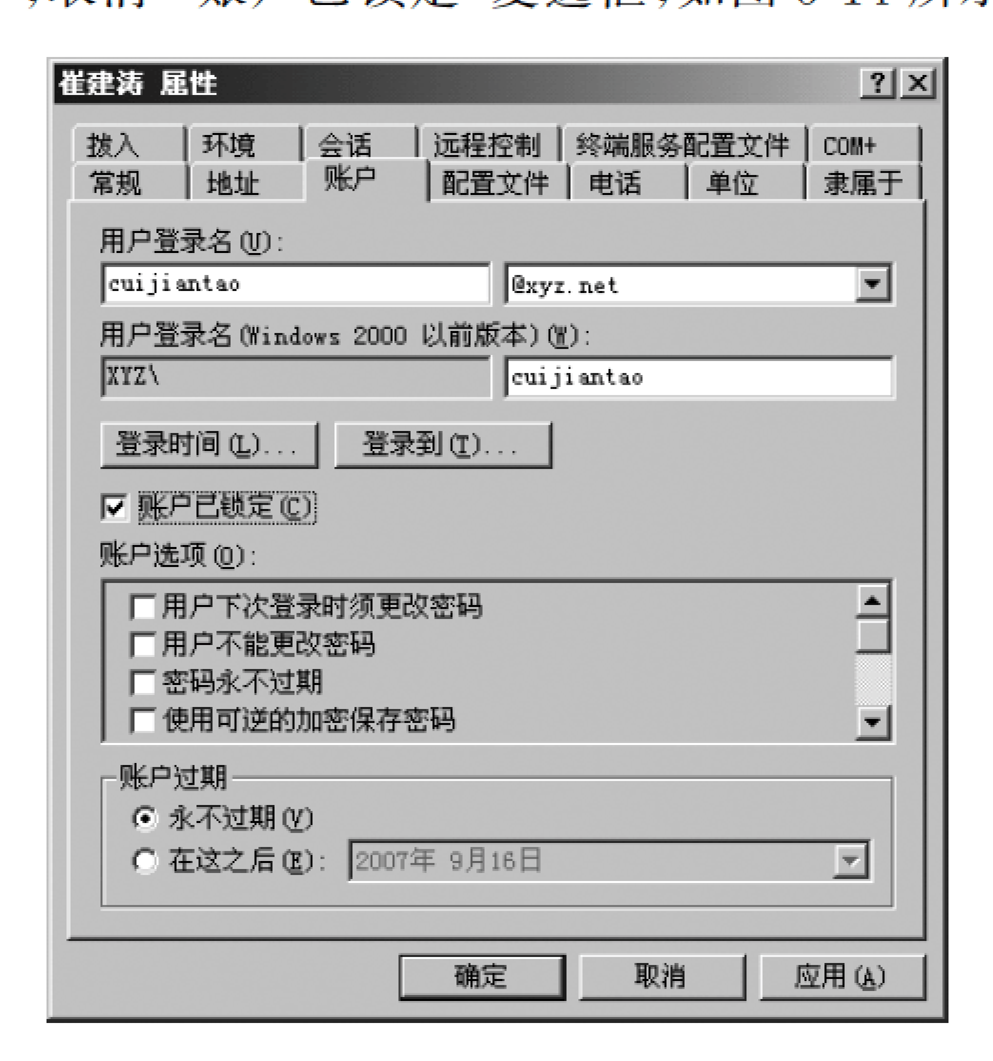


图 5-14 解除被锁定的账户

说明：在创建一个用户账户时，系统都会为其建立唯一的安全识别码（SID），Windows Server 2003 利用这个 SID 来代表该用户，而权限的设置等都是通过 SID 设置的，并不是通过用户的账户名称，例如，某个文件的权限列表内，记录的是哪些 SID 具备什么权利，而不是哪些用户账户名称具备何种权利。因此，在重命名账户名称后，由于 Windows Server 2003 内部代表该用户的 SID 并没有被改变，因此其账户的属性、权利与权限等都不变。在删除一个账户后，即使再添加一个相同名称的账户，这个新账户并不会继承原账户的权限、权利与组关系。

5.5.3　用户配置文件

Windows 2003 要求访问计算机的每个用户账户都要有一个独立的用户配置文件，用户配置文件包含用户所使用的计算机的显示设置、区域设置、鼠标设置、声音设置、网络设置以及打印机等工作环境的设置。用户的桌面环境主要由用户配置文件决定。管理员可以为用户定制用户配置文件来统一用户的桌面环境与工作环境，例如，使用户在每次登录计算机时，都有相同的桌面、相同的网络驱动器、相同的网络打印机等。

1. 用户配置文件的类型

用户配置文件的类型有以下 4 种。

（1）默认用户配置文件。它是所有用户配置文件的基础。每个用户配置文件最初都是以默认用户配置文件为基础而创建的，默认用户配置文件存储在每台运行 Windows Server 2003 计算机的%systemdrive%\Documents and Settings\Default User 文件夹中。

（2）本地用户配置文件。用户第一次登录某台计算机时，系统就会自动为该用户在这台计算机内创建一个本地用户配置文件。当用户注销时，其对桌面的任何更改都会更新到本地用户配置文件内。下次用户登录时，就会应用这个更新过的本地用户配置文件。

（3）漫游用户配置文件。漫游用户配置文件使域中的用户不论在域内的哪一台计算机上登录，都能够拥有相同的桌面设置。漫游用户配置文件由系统管理员创建并存储到服务器上。当用户注销时，其对桌面的任何更改都会更新到漫游用户配置文件中。下次用户登录时，就会应用这个更新过的漫游用户配置文件。

（4）强制用户配置文件。强制用户配置文件由系统管理员事先创建并存储在服务器上，用户登录后可以更改其桌面设置，但是当用户注销时，对桌面的这些更改并不会更新到强制用户配置文件内。因此，用户每次登录时使用的是固定不变的桌面设置。只有系统管理员可以对强制用户配置文件的设置进行更改。

2. 用户配置文件的组成

用户配置文件并不是单纯的一个文件，而是由用户配置文件与文件夹、NTUSER.DAT 文件、All Users 文件夹 3 个部分决定。

1）用户配置文件、文件夹

用户配置文件、文件夹包含用户的桌面、收藏夹、我的文档、开始菜单等设置。图 5-15

显示了用户 cuijiantao 的用户配置文件、文件夹的内容。

图 5-15　用户配置文件、文件夹的内容

关于用户配置文件、文件夹中更多的内容，如表 5-4 所示。

表 5-4　用户配置文件、文件夹的内容

用户配置文件、文件夹	内　　容
「开始」菜单	「开始」菜单内各程序的快捷方式
Application Data	应用程序专用的数据，例如客户数据文件。由应用程序供应商决定在包含用户配置文件的文件夹中保存哪些数据
Cookies	用户信息和首选项
My Documents	用户的个人文件存储区
Local Settings	应用程序的相关数据、历史和临时文件等
NetHood	“网上邻居”的快捷方式
PrintHood	打印机文件夹的快捷方式
Recent	最近最常用的文件与文件夹的快捷方式
SendTo	用户右击任何文件→“发送到”所出现的菜单的快捷方式
Templates	用户模板项目的快捷方式
收藏夹	Internet Explorer 收藏夹的快捷方式
我的最近文档	用户最近打开的文档
桌面	桌面上的项目，包含文件、文件夹与快捷方式

2）NTUSER.DAT 文件

NTUSER.DAT 文件包含注册表中用于用户账户的部分也包含用户配置文件设置。用户配置文件内的当前登录用户的环境设置数据存储在注册表的 HKEY_CURRENT_USER 内，例如已安装的软件、桌面、网络连接等。

3）All Users 文件夹

用户配置文件的第 3 部分数据存储在 All Users 文件夹中，如图 5-15 中用圆圈标注的部分，登录这台计算机的所有用户都会使用包含在这个文件夹内的「开始」菜单、“桌面”等设置。

3. 本地用户配置文件

当用户第一次登录 Windows Server 2003 计算机时，系统就会自动为该用户在这台计算机的 Documents and Settings 文件夹内创建一个以用户账户命名的“本地用户配置文件”文件夹，以用来存储该用户的桌面设置，其内容由复制“默认用户配置文件”文件夹而来。

事实上，首次登录这台计算机的任何一个用户的桌面环境，都是由 Default User 文件夹与 All Users 文件夹内的内容组合而成。当用户注销时，其所做的任何设置上的更改都会存储到这个本地用户配置文件与文件夹内，用户下次重新登录时，就会以这个本地用户配置文件与文件夹的内容（组合 All Users 文件夹的内容）设置其桌面环境。在整个过程中，Default User 文件夹的内容并不会受任何影响。

同一个用户在不同的计算机内有其不同的本地用户配置文件，一台计算机上允许存在多个用户的本地用户配置文件。例如，图 5-15 中的 Administrator、cuijiantao 等文件夹都是本地用户配置文件、文件夹。

系统管理员可以单击“开始”→“控制面板”→“系统”→“高级”→“用户配置文件”，或者单击“开始”，右击“我的电脑”→“属性”→“高级”→“用户配置文件”，查看当前的计算机内有哪些用户配置文件，如图 5-16 所示。

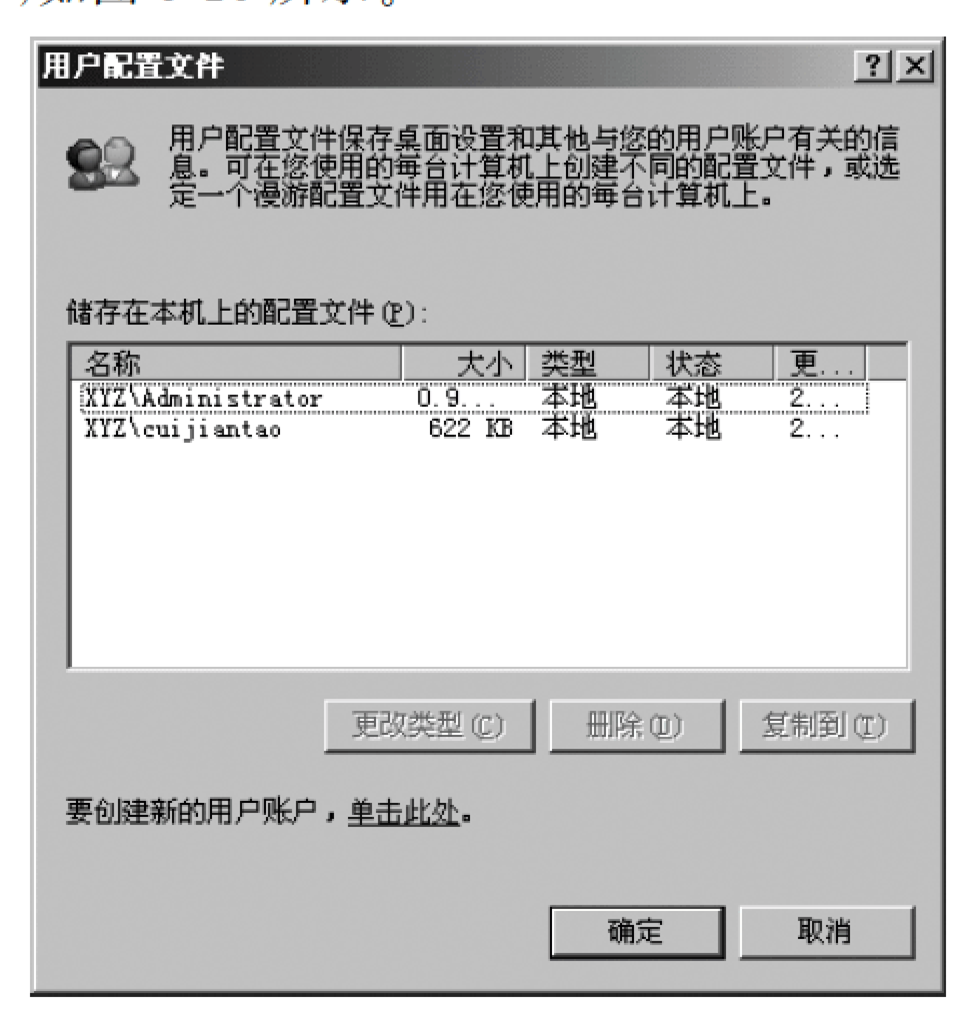


图 5-16　查看本机上储存的用户配置文件

4. 漫游用户配置文件

漫游用户配置文件由系统管理员创建并存储到服务器上。漫游用户配置文件使得域中的用户不论从域内的哪一台计算机登录，都能够读取到这个用户配置文件，使用相同的桌面设置。当用户注销时，其对桌面的任何更改都会更新到漫游用户配置文件中，用户下次重新登录时，就会应用这个更新过的漫游用户配置文件。

如果用户要求无论从域内的哪一台计算机登录都能够拥有相同的工作环境，管理员就可以指定用户使用漫游用户配置文件。

要指定用户使用漫游用户配置文件，可以通过以下两种方式。

(1) 给用户指定一个空的漫游用户配置文件。

(2) 给用户指定一个自定义的漫游用户配置文件。

当需要为多个职责相似的用户提供一个标准的桌面环境时，或者需要删除用户不需要的连接和应用程序时，最好使用自定义的漫游用户配置文件。

1) 给用户指定一个空的漫游用户配置文件

假设要给域用户 cuijiantao 指定一个空的漫游用户配置文件，并将这个漫游用户配置文件存储在服务器 server01 的共享文件夹 User_profiles 内，则操作步骤如下。

(1) 在服务器 server01 上创建一个文件夹 User_profiles，并设为共享，共享名为 User_Profiles，设置 Everyone 组对该文件夹至少要有"更改"的共享权限。

(2) 利用 Domain Admins 或者 Enterprise Admins 组成员的身份登录，打开"Active Directory 用户和计算机"，展开用户账户 cuijiantao 所在的组织单位，右击"崔建涛"→"属性"，单击如图 5-17 所示的"配置文件"选项卡→在"配置文件路径"处，输入漫游用户配置文件的 UNC 路径\\server01\User_profiles\cuijiantao，或者\\server01\User_profiles\%username%。其中 server01 为服务器的名称，User_profiles 共享文件夹的共享名，

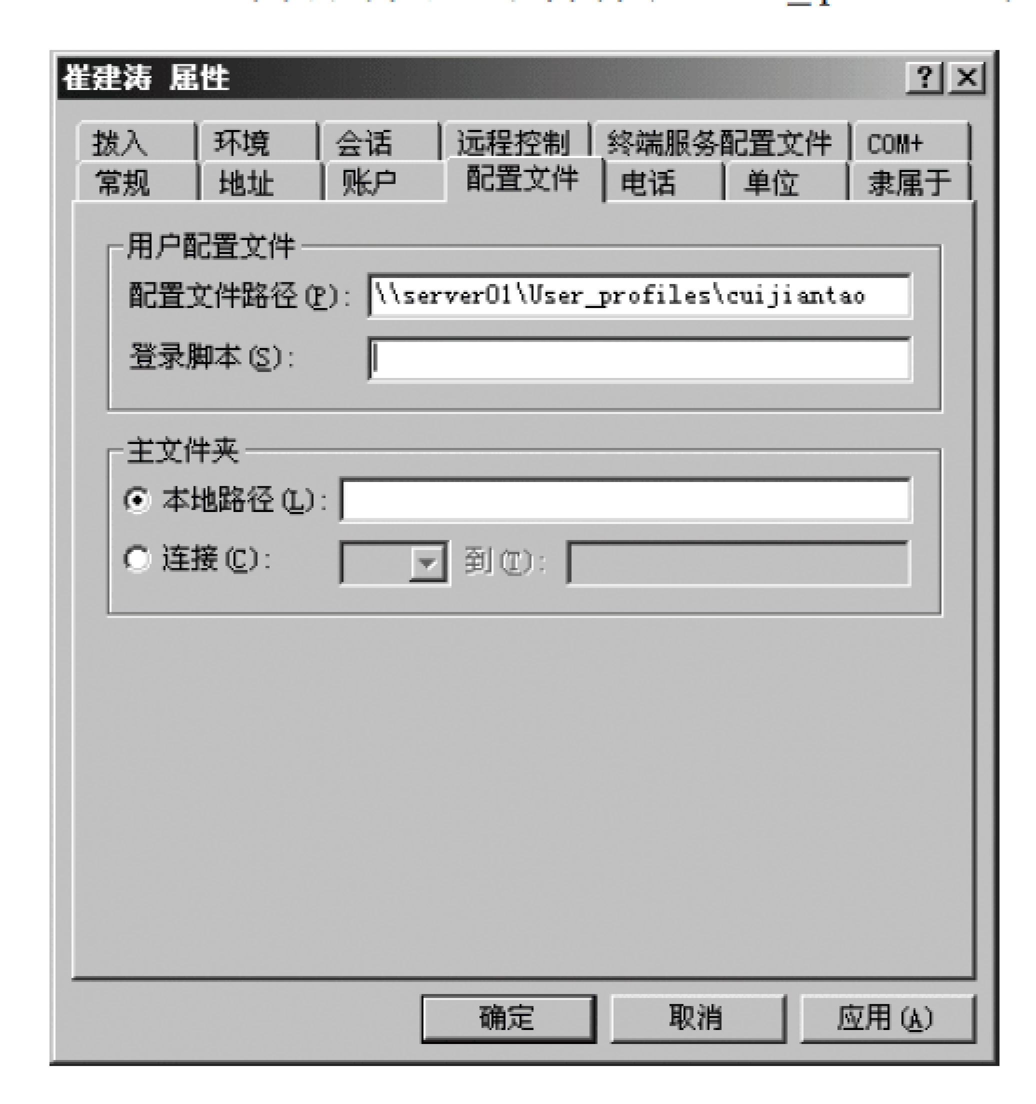


图 5-17 输入漫游用户配置文件的 UNC 路径

cuijiantao 为漫游用户配置文件、文件夹名称(建议与用户账户名称同名,该文件夹不需要手工创建),可以使用变量%username%来代替输入文件夹名,系统会自动把 UNC 路径中的%username%替换为该用户的账户名。完成后,单击“确定”按钮。

完成后,当用户 cuijiantao 从域内的任何一台计算机上登录时,系统就会自动为该用户在服务器上创建一个漫游用户配置文件、文件夹,不过此时该文件夹中尚未包含任何内容。当用户注销时,其对桌面设置所做的任何更改(例如,更改桌面背景)将被存储到该漫游用户配置文件中,同时也会存储到本地用户配置文件中。以后该用户无论是从网络上的哪一台计算机登录到域,都会读取这个漫游用户配置文件,并以这个用户配置文件的内容设置其桌面环境。

2) 给用户指定一个自定义的漫游用户配置文件

假设要给域用户 wangwu 指定一个管理员自定义的漫游用户配置文件,并将这个漫游用户配置文件存储在服务器 server01 的共享文件夹 User_profiles 内,则操作步骤如下。

首先创建一个自定义的漫游用户配置文件,分为以下 3 个步骤。

(1) 利用一个临时的域用户账户(例如 template,请事先在域控制器上创建该域用户账户),从域内的任何一台计算机(例如 pc01)上登录到域。成功登录后,系统会为该账户创建一个本地用户配置文件,对应的本地用户配置文件存储在本地计算机(例如 pc01)上,这个用户配置文件将作为管理员要自定义的漫游用户配置文件的基础模板。

(2) 更改其桌面环境,例如,更改桌面背景、网络驱动器、网络打印机、安装应用程序等。

(3) 注销当前的用户,使这些更改存储到此临时账户的本地用户配置文件中。

接下来,将创建的本地用户配置文件复制到服务器 server01 上,并将其指定给用户 wangwu 使用,操作步骤如下。

(1) 在服务器 server01 上创建一个文件夹 User_profiles,并设为共享,共享名为 User_profiles,设置 Everyone 组对该文件夹至少要有“更改”的共享权限。

(2) 利用 Domain Admins 或 Enterprise Admins 组成员的身份,从域内的成员计算机(例如 pc01)登录到域,单击“开始”→“控制面板”→“系统”→“高级”,单击“用户配置文件”中的“设置”按钮。

(3) 出现图 5-18 时,选择账户 XYZ\template,单击“复制到”按钮。

(4) 出现图 5-19 时,执行操作如下。

① 在“将配置文件复制到”下的文本框中输入存储漫游用户配置文件的 UNC 路径\\server01\User_profiles\wangwu,其中 server01 为域控制器名称,User_profiles 为共享文件夹名称,wangwu 为漫游用户配置文件的文件夹名称(建议与用户账户名称同名,该文件夹不需要手工创建)。

② 单击“允许使用”内的“更改”,使用户 wangwu 有权访问此漫游用户配置文件、文件夹。

(5) 返回“用户配置文件”对话框,单击“确定”按钮即可。

(6) 在域控制器 server01 上,打开“Active Directory 用户和计算机”,展开用户账户

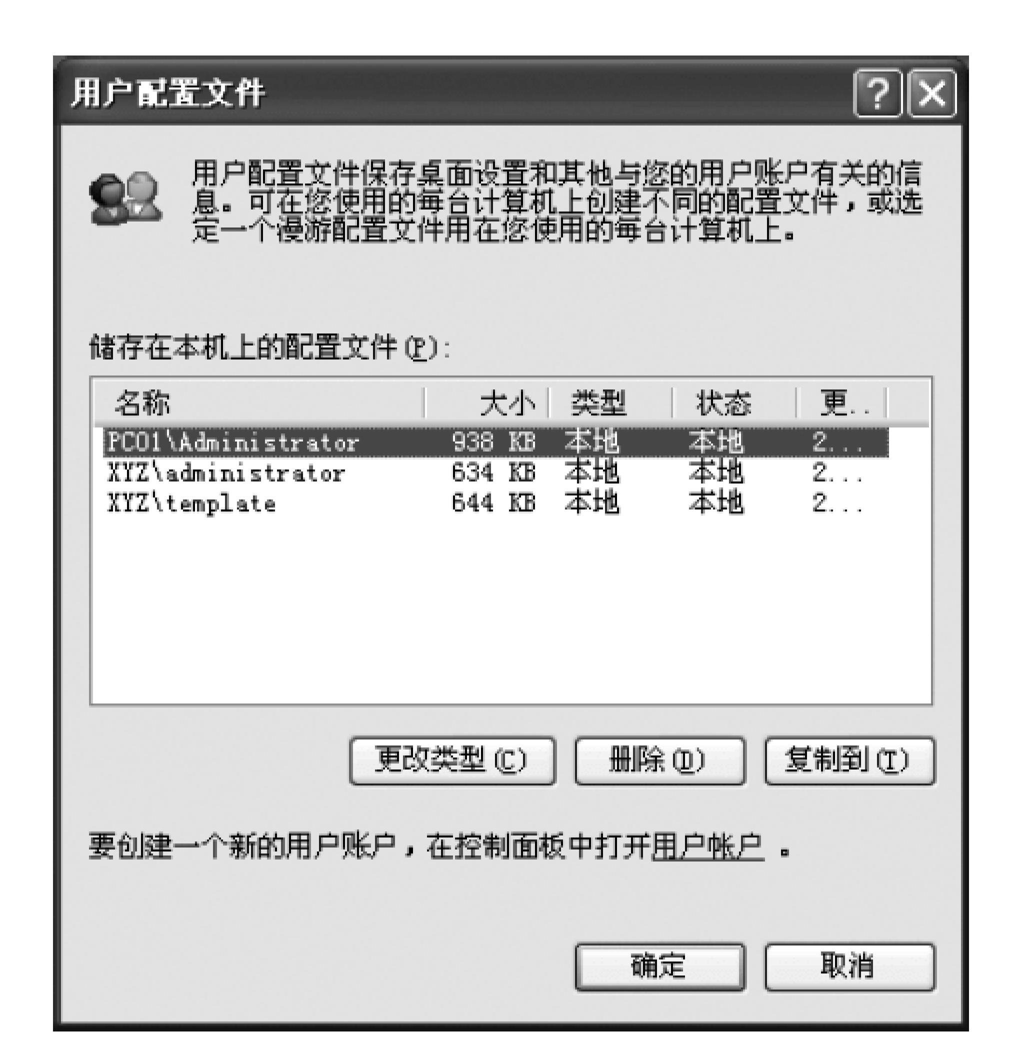


图 5-18 复制用户配置文件



图 5-19 指定复制的目标路径

wangwu 所在的组织单位，右击“王武”→“属性”→“配置文件”选项卡，在如图 5-20 所示对话框中的“配置文件路径”处，输入漫游用户配置文件的 UNC 路径\\server01\User_profiles\wangwu，或者\\server01\User_profiles\%username%。其中 server01 为域控制器的计算机名称，User_profiles 为共享文件夹的共享名，wangwu 为漫游用户配置文件的文件夹名称。可以使用变量%username%来代替输入文件夹名，Windows 2003 会自动把 UNC 路径中的%username%替换为该用户的账户名

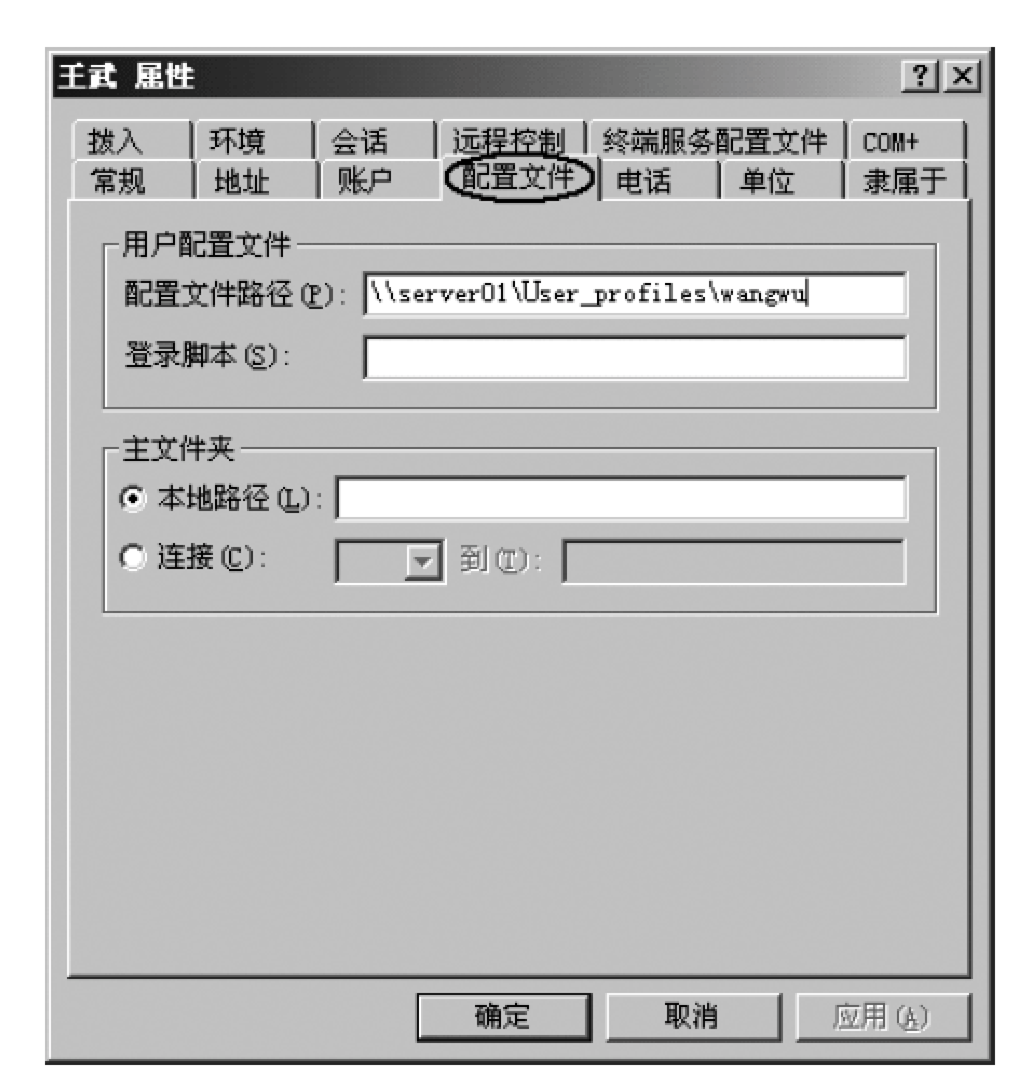


图 5-20 输入用户配置文件的路径

(7) 完成后，单击“确定”按钮。

当用户 wangwu 从域内的任何一台计算机登录到域时，就会自动读取存储在服务器

上的 user_profiles 共享文件夹中的漫游用户配置文件，并以这个用户配置文件的内容来设置其桌面环境。当用户注销时，其对桌面设置所做的任何更改（例如更改桌面背景）会存储到该漫游用户配置文件内，同样也会存储到用户所使用的计算机的本地用户配置文件内。

5. 漫游用户配置文件的操作过程

使用漫游用户配置文件的用户在登录到域时，其计算机会读取存储在服务器上的漫游用户配置文件，以便根据该用户配置文件来决定用户的桌面环境。而当用户注销时，用户的桌面设置会被同时存储到漫游用户配置文件与本地用户配置文件内。

如果用户在登录域时，因故无法访问位于服务器内的漫游用户配置文件，例如网络故障、安全权限不足等，则会出现图 5-21。

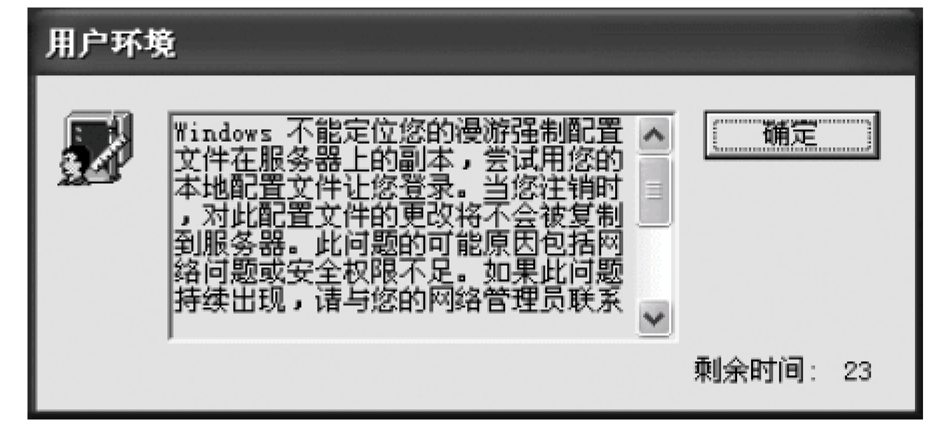


图 5-21　不能定位漫游配置文件

此时，系统将会使用哪个用户配置文件登录呢？有以下两种情况。

（1）如果用户是第一次从这台计算机上登录，则因为该计算机内当前还没有该用户的本地用户配置文件，因此系统会以 Default User 配置文件的内容设置用户的环境。当用户注销时，其桌面设置既不会被存储到服务器上的漫游用户配置文件内，也不会被存储到本地用户配置文件内。

（2）如果用户以前从该计算机上登录过，则将使用他在该计算机内的本地用户配置文件。当用户注销时，其桌面设置并不会被存储到服务器上的漫游用户配置文件内，只会被存储到本地用户配置文件文件夹内。而当用户下一次登录到域时，即使此时网络故障、安全权限不足等问题已经解决，也就是已经可以正常地访问服务器上的漫游用户配置文件，但是由于本地用户配置文件的数据比较新，因此仍然会使用本地用户配置文件，不过注销时，就可以正常地将最新的桌面设置存储到漫游用户配置文件内了。

用户在登录时，系统会比较服务器上的漫游用户配置文件与本机内的本地用户配置文件，两者之间哪个比较新（利用日期与时间进行比较），再决定使用哪个用户配置文件，使用的规则如下。

（1）如果本地的比较新，则读取本地用户配置文件。

（2）如果服务器上的比较新，则读取服务器上的漫游用户配置文件。

（3）如果两者是相同的，则直接使用本地用户配置文件，从而提高读取效率。

无论系统使用哪个用户配置文件，当用户注销时，其环境的更改都会存储到这两个用户配置文件内。

6. 强制用户配置文件

强制用户配置文件事先由系统管理员创建并存储在服务器上，用户登录后可以更改其桌面设置，但是当用户注销时，对桌面的这些更改并不会更新到强制用户配置文件内。因此用户每次登录时使用的是固定不变的桌面设置。系统管理员可以更改强制用户配置

文件的设置。

使用强制用户配置文件时,用户对桌面设置的更改虽然不会存储到服务器上,但会存储到本机上的本地用户配置文件内。用户下一次登录时,如果服务器上的强制用户配置文件因故无法访问时,则会使用本地用户配置文件。

创建强制用户配置文件的方法与创建漫游用户配置文件一样,区别在于,系统管理员必须将这个漫游用户配置文件、文件夹内的 ntuser. dat 文件名修改为 ntuser. man,这样漫游用户配置文件就变成了强制用户配置文件了,如图 5-22 所示。



图 5-22 修改漫游用户配置文件为强制用户配置文件

如果有一组用户(例如公司的会计)需要使用相同的桌面设置,而管理员又不希望这些用户更改其桌面,此时管理员可以为这些用户指定同一个强制用户配置文件。

5.5.4 用户主文件夹

默认情况下,每个用户的个人文档保存在"我的文档"文件夹内,而"我的文档"文件夹是用户配置文件的一部分。如果用户使用的是存储在服务器上的漫游用户配置文件,则用户在登录时会从服务器上读取"我的文档"里的内容。当用户注销时,也会把"我的文档"里的内容保存到服务器上,这将会降低用户登录或注销的效率。

要解决上述问题,可以修改"我的文档"的存储位置,操作步骤为:单击"开始",右击"我的文档"→"属性"→"目标文件夹",修改"我的文档"目标文件夹的位置,如图 5-23 所示。

除了"我的文档"外,Windows Server 2003 还提供了另一个集中存储个人文档的网络位置,这就是用户的主文件夹。由于用户的主文件夹不是用户配置文件的一部分,所以它不会影响用户的登录过程。

要将域用户 wangwu 的主文件夹定向到服务器 server01 的共享文件夹 User_docs



图 5-23 修改"我的文档"目标文件夹的位置

内,设置其主文件夹的操作步骤如下。

(1) 利用域管理员账户登录到域控制器 server01。

(2) 在域控制器 server 01 上,创建文件夹 User_docs,并将其设置为共享,共享名为 User_docs,并设置域管理员至少具有"更改"的共享权限。

(3) 打开"Active Directory 用户和计算机",单击用户账户 wangwu 所在的组织单位,右击用户账户"王武(wangwu)"→"属性"→"配置文件"选项卡。

(4) 在图 5-24 中,选择主文件夹中的"连接…到",并输入主文件夹的 UNC 路径\\server01\User_docs\wangwu,或者\\server01\User_docs\%username%。其中 server01

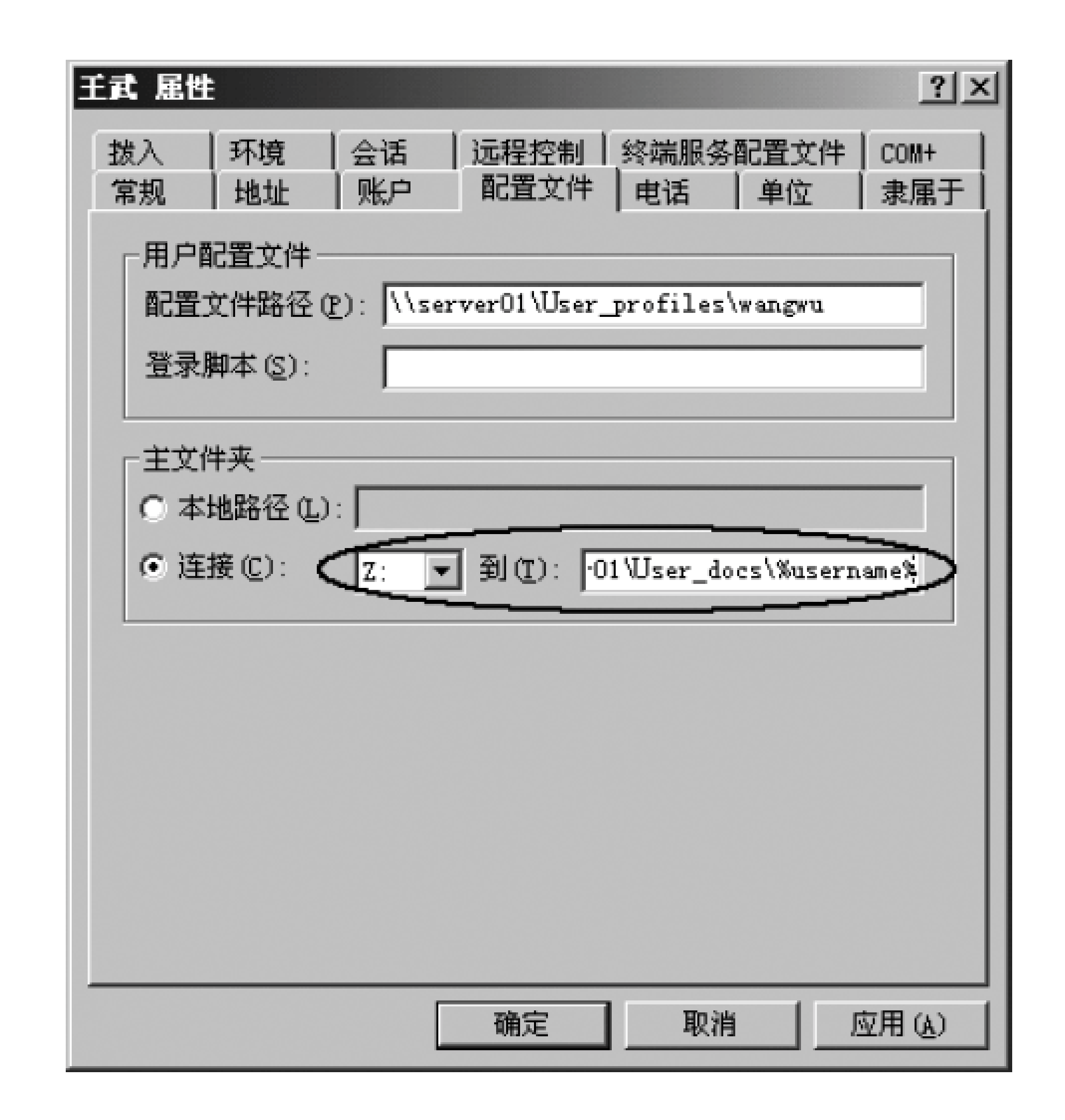


图 5-24 设置主文件夹的路径

为域控制器的名称，User_docs 为共享文件夹的共享名，wangwu 为该用户的主文件夹名称(建议与用户账户同名，该文件夹不需要手工创建)，可以使用变量%username%来代替输入主文件夹名称，Windows 2003 会自动把 UNC 路径中的%username%替换为该用户的账户名。完成后，单击"确定"按钮。

服务器端的设置完成后，当王武(wangwu)从域内的任何一台计算机登录到域后，打开"我的电脑"，会出现一个网络驱动器 Z，该驱动器会自动连接到该用户的主文件夹\\server01\User_docs\wangwu，以后王武就可以将其个人文档存储到网络驱动器 Z 上的主文件夹了，如图 5-25 所示。



图 5-25 客户端使用主文件夹

建议把用户的"我的文档"重定向到此用户对应的"主文件夹"的位置，可以进一步增强主文件夹的功能。

5.6 组账户的工作方式

组是用户账户的集合。管理员可以一次性为组授予访问共享资源的权限，而不用分别为每个用户授予权限。组的应用简化了对用户的管理，减轻了网络管理员的负担。

出于企业的用途或者管理任务的需要，管理员除了可以将用户账户添加为组的成员外，也可以将其他计算机甚至其他组添加为组的成员。在添加组的成员时，需要考虑以下情况。

(1) 当将一个用户账户添加为组的成员时，该账户就被授予了该组拥有的所有权限

(2) 一个用户账户可以是多个组的成员。

Windows 2003 本身提供了具有特定权限的内置组，可以通过把用户添加到这些内置组中来简单地实现组。Windows 2003 也提供了一些常见的策略使管理员或者用户更有效地创建和使用组。

5.7 本地组

5.7.1 本地组概述

本地组也就是在工作组中实现的组。本地组可以在 Windows Server 2003/Windows 2000/Windows NT 独立服务器或成员服务器、Windows XP Professional/Home Edition、Windows NT Workstation 等非域控制器的计算机上创建。

只有 Administrator 组或者 Power Users 组的成员才有权创建本地组。创建的这些组账户被存储在这些计算机的"本地安全账户数据库"内。

只能在创建本地组的计算机上使用本地组，换句话说，本地组只能够用来控制本地计算机上资源的访问或用来对本地计算机执行系统任务。管理员需要分别在每台计算机上管理本地组。

提示：不建议在隶属于域的客户端计算机或成员服务器上创建、使用本地组，这样做不利于域的集中管理。

本地组只能包括创建该本地组的计算机上的本地用户账户。但是如果该计算机是域的成员，那它也可以包含该计算机所属域或所信任域内的域用户账户、全局组和通用组。本地组不能是其他任何组的成员。

除了用户创建本地组之外，Windows Server 2003 本身提供了拥有在本地计算机上执行系统任务的特定权限的内置组，内置组不能被删除。内置组包括内置本地组和内置的特殊组，关于内置的特殊组，在 5.8 节中介绍。这些内置组拥有一组预定义的权限，这些权限决定了用户可以执行哪些系统任务。

表 5-5 描述了最常用的内置本地组及其描述。

表 5-5 最常用的内置本地组及其描述

本 地 组	描 述
Users	该组内的成员只拥有一些基本的权利，例如运行应用程序，但是不能修改操作系统的设置、不能更改其他用户的数据、不能关闭服务器级的计算机。所有添加的本地用户账户都自动属于该组。如果这台计算机已加入域，则域的 Domain Users 会自动隶属于该计算机的 Users 组
Administrators	该组内的用户具备系统管理员的权限，拥有管理这台计算机的最大权限。内置的系统管理员账户 Administrator 就是该组的成员。如果这台计算机已加入域，则域的 Domain Admins 会自动地加入到该计算机的 Administrators 组内。也就是说，域中的系统管理员也具备这台计算机上系统管理员的权限
Guests	Guests 组提供给需要访问本地计算机内的资源但又没有用户账户的用户使用。该组的成员无法永久改变其桌面的工作环境，默认成员为用户账户 Guest，该账户默认是被禁用的。如果这台计算机已加入域，则域的 Domain Guests 会自动地被加入到该计算机的 Guests 组中

续表

本地组	描述
Backup Operators	该组内的成员不论是否有权访问这台计算机中的文件或文件夹，都可以通过 Windows 提供的备份工具，备份与还原这些文件或文件夹
Power Users	该组内的用户具备比 Users 组更多的权利，但是比 Administrators 组更少的权利，例如，可以在本地计算机上创建、删除、管理本地用户账户、共享文件夹、共享打印机等，也可以自定义系统设置，例如，更改计算机时间、关闭计算机等。Power Users 组的成员不可以更改 Administrators 与 Backup Operators、无法获取文件的所有权、无法备份与还原文件、无法安装与删除设备驱动程序、无法管理安全与审核日志
Replicator	该组内的成员可以配置文件复制服务
Network Configuration Operators	该组内的用户可以在客户端执行一般的网络设置任务，例如更改 IP 地址，但是不可以安装/删除驱动程序与服务，也不可以执行与网络服务器设置有关的任务，例如 DNS 服务器、DHCP 服务器的设置
Remote Desktop Users	该组的成员可以通过远程计算机登录，例如，利用终端服务器从远程计算机登录

5.7.2 在工作组中使用本地组的策略

在工作组环境中，用户要想获取访问某台计算机上的共享资源的权限或者对该计算机执行系统管理任务，则该用户在这台计算机上必须有一个本地用户账户。如果计算机上的多个用户要求访问相同的资源或者执行同样的系统管理任务，就可以使用本地组来授予权限，然后把相应的用户账户添加为本地组的成员。这种方法称为 ALP 策略，即把用户账户(A)添加到本地组(L)里，授予计算机上的本地组相应的权限(P)。

提示：如果把用户账户添加到系统的内置组中，就可以达到授予用户权限的目的，就不必再另外创建一个新的本地组。

5.7.3 创建本地组

在 Windows Server 2003 上，创建本地组的操作步骤如下。

(1) 单击“开始”→右击“我的电脑”→选择“管理”，或者单击“开始”→选择“管理工具”→打开“计算机管理”→展开“本地用户和组”→右击“组”→选择“新建组”，如图 5-26 所示。

(2) 在图 5-27 中，输入组名，例如“L_市场部”。也可以单击“添加”→“高级”→“立即查找”来添加组的成员。完成后，单击“创建”按钮即可。



图 5-26　新建本地组



图 5-27　添加本地组的成员

5.8　域组

域中的组存储在 Active Directory 数据库内。使用域中的组，管理员能够更好地组织域中的用户，并实施资源的访问权限控制。在域中使用组有更多的选项，理解相应的使用策略很重要。

5.8.1　域组概述

Windows Server 2003 的 Active Directory 内包含了许多内置的组，包含本地域组、全

局组和特殊组，这些内置组分别如下。

1. 内置的本地域组

Windows Server 2003 域控制器的活动目录中的 Builtin 容器内已经内置了一些本地域组，如表 5-6 所示。这些组已经被赋予了一些权利与权限，以便让其能够管理整个域与活动目录。只要将用户账户或组账户添加到这些内置的本地域组中，这些账户也将具备与内置的本地域组相同的权利与权限。

表 5-6 常用的本地域组

内置的本地域组	描　　述
Account Operators	系统默认该组内的成员可以在除 Builtin 容器与 Domain Controller 组织单位以外的任何一个容器与组织单位内新建、删除、更改用户账户、组账户、计算机账户。但无法更改或删除 Administrators 与 Domain Admins 组的成员
Administrators	该组内的成员具备系统管理员的权限，拥有管理整个域控制器(活动目录)最大的权限。该组的默认成员包含内置的系统管理员账户 Administrator、Domain Admins 全局组、Enterprise Admins 全局组等
Backup Operators	该组的成员可以备份与还原域控制器内的文件夹与文件，还可以关闭域控制器
Guests	该组是供没有用户账户、但又需要访问资源的用户使用，该组的成员无法永久地改变其桌面的工作环境。该组默认的成员为用户账户 Guest 与全局组 Domain Guests
Network Configuration Operators	该组内的用户，可以在域控制器上进行一般的网络设置工作，例如，更改 IP 地址，但是不可以安装/删除驱动程序与服务，也不可以执行与网络服务器设置有关的任务，例如 DNS 服务器、DHCP 服务器的设置
Pre_Windows 2000 Compatible Access	该组主要是为了与 Windows NT 4.0 计算机(或更旧的计算机)兼容。其成员可以读取 Windows Server 2003 域中的所有用户与组账户。其默认的成员为特殊组 Authenticated Users。只有在用户所使用的计算机是 Windows NT 4.0 或更旧的系统时才将用户加入到该组中
Printer Operators	该组的成员可以创建、停止或管理域控制器上的共享打印机，也可以关闭域控制器
Remote Desktop Users	该组的成员可以通过远程计算机登录，例如利用终端服务器从远程计算机登录
Server Operators	该组的成员可以创建、管理、删除域控制器上的共享文件夹与打印机；备份与还原域控制器内的文件；锁定与解开域控制器；将域控制器上的硬盘格式化；更改域控制器的系统时间；关闭域控制器等
Users	该组的组员只拥有一些基本的权限，例如运行应用程序，但是他们不能修改操作系统的设置，不能更改其他用户的数据，不能关闭服务器级的计算机。该组默认的成员为 Domain Users 全局组

2. 内置的全局组

当创建一个域时，系统会在活动目录中的 Users 容器内创建一些内置的全局组，如表 5-7 所示。这些全局组本身并没有任何权利与权限，但是可以将其添加到本地域组中来

获取相应的权利或权限，或者直接给该全局组指派权利或权限。

表 5-7 常用的全局组

内置的全局组	描 述
Domain Admins	域内的成员计算机会自动地将该组加入到其 Administrators 组中，因此该组内的每个成员都具备系统管理员的权限。该组默认的成员为域用户 Administrator
Domain Computers	所有加入到该域的计算机都自动隶属于该组
Domain Controllers	域内的所有域控制器都自动隶属于该组
Domain Users	域内的成员计算机会自动地将该组加入到其 Users 组内。该组默认的成员为域用户 Administrator，以后添加的所有域用户账户都自动隶属于该组
Domain Guests	系统会自动地将该组加入到 Guests 本地域组内。该组的默认成员为用户账户 Guest
Enterprise Admins	该组只存在于整个域目录林的根域中，其成员具有管理整个域目录林内的所有域的权利。该组的默认成员为域目录林根域内的用户 Administrator
Schema Admins	该组只存在于域目录林的根域中，其成员具备管理构架的权利。该组的默认成员为域目录林根域内的用户 Administrator

3. 内置的特殊组

特殊组也称为系统组，存在于所有运行 Windows Server 2003 的计算机内，如表 5-8 所示，这些组自动为特定的系统用途组织用户。管理员不能更改这些组的成员身份，也就是说，无法在“Active Directory 用户和计算机”或“计算机管理”内看到、管理这些组。这些组只有在设置权利、权限时才看得到。

表 5-8 常用的特殊组

内置的特殊组	描 述
Everyone	任何一个用户(包括 Guest 用户)都隶属于这个组。当一个没有账户的用户连接计算机时，如果 Guest 账户被启用时，他将自动利用 Guest 账户连接，也将具备 Everyone 拥有的权限。因此，给 Everyone 组指派权限时要十分小心
Authenticated Users	任何一个利用有效的用户账户连接的用户都隶属于这个组。建议在设置权限时，尽量针对 Authenticated Users 组进行设置，而不要针对 Everyone 组进行设置
Interactive	任何在本地登录的用户都隶属于这个组
Network	任何通过网络连接到此计算机的用户都隶属于这个组
Creator Owner	文件夹、文件或打印文件等资源的创建者，就是该资源的 Creator Owner(创建者/所有者)。如果创建者是 Administrators 组内的成员，则其 Creator Owner 为 Administrators 组
Anonymous Logon	任何未利用有效的用户账户连接的用户都隶属于这个组
Dialup	任何利用拨号方式连接的用户都隶属于这个组

用户要么默认就是这个组的成员，要么在网络操作过程中成为这个组的成员。例如，用户登录一台计算机并且获得该计算机上资源的访问权，在登录这一操作过程中，该用户就成了 Interactive 特殊组的成员。

5.8.2 域组类型和作用域

1. 组的类型

组的类型决定了可以用这个组管理的任务的类型，有以下两种类型。

(1) 安全组。安全组用来实现与安全有关的目的，被授予访问资源的权限。安全组也可以用在与安全无关的任务上，例如，可以使用安全组向多个用户发送电子邮件消息，向安全组发送电子邮件消息就是向该组的所有成员发送这个消息，因此安全组共享通信组的功能。

(2) 通信组。通信组用来实现与安全(权限的设置等)无关的任务，例如，向一组用户发送电子邮件。通信组不能被授予访问资源的权限。即使安全组有通信组的全部功能，通信组仍是必需的，因为一些应用程序只能读取通信组。

在域功能级别为“Windows 2000 纯模式”或者 Windows Server 2003 时，安全组与通信组之间可以互相转换，在域功能级别为“Windows 2000 混合模式”时无法转换。

2. 组的作用域

组的作用域决定了这个组是跨多个域还是限制在单个域中，决定了在域的何处可以使用组，例如，有的组仅可在所属的域中使用，而有的组可在整个域目录林中的所有域中使用。组的作用域也影响组成员身份和组的嵌套。组的嵌套就是把一个组作为成员添加到另一个组里。

根据组的作用域，Windows Server 2003 域中的组分为通用组、全局组、本地域组 3 种。关于这些组的特性，分别介绍如下。

1) 通用组

(1) 通用组拥有开放的成员身份，通用组的成员能够包含整个域目录林中任何一个域内的用户、通用组、全局组。但无法包含任何一个域内的本地域组。

(2) 允许把通用组添加到任何域中的本地域组或者通用组里。

(3) 通用组可以访问任何一个域内的资源，也就是说，可以在任何一个域内为通用组(这个通用组可以在该域中，也可以在另一个域中)授予访问资源的权限。

2) 全局组

(1) 全局组主要用来组织用户，也就是可以将多个即将被赋予相同权限的用户账户加入到同一个全局组中。

(2) 全局组拥有有限的成员身份，全局组的成员只能够包含与该全局组在同一个域中的用户与全局组。

(3) 允许把一个全局组添加到同一个域中的另一个全局组，或者位于同一个域，或者

其他域中的通用组和本地域组里。

(4) 全局组可以访问任何一个域中的资源,也就是说,可以在任何一个域内为全局组授予访问资源的权限(这个全局组可以在同一个域,也可以在另一个域中)。

3) 本地域组

(1) 本地域组拥有开放的成员身份,本地域组的成员,能够包含任何一个域内的用户、通用组、全局组;它还能够包含同一个域内的本地域组;但是它无法包含其他域内的本地域组。

(2) 本地域组只能够访问该本地域组所在的域内的资源,无法访问其他不同域内的资源。也就是说,只能把本地域组所在域内的资源的访问权限授予给本地域组。

关于各种域组的特性对比,如表 5-9 所示。

表 5-9 各种域组的特性对比

特性\组	通 用 组	全 局 组	本 地 域 组
成员(Windows 2000 混合模式)	不支持通用组(组类型是“通信组”除外)	同一个域内的用户账户和计算机账户	所有域内的用户账户、计算机账户和全局组
成员(Windows 2000 纯模式或 Windows Server 2003)	所有域内的用户账户、计算机账户、全局组、通用组	同一个域内的用户账户、计算机账户和全局组	所有域内的用户账户、计算机账户、全局组、通用组;同一个域内的本地域组
可以指派哪一个域内资源的访问权限	所有域(域功能级别必须是 Windows 2000 纯模式或 Windows Server 2003)	所有域	同一个域
组转换	可转换为本地域组;可转换为全局组(只要该组不包含通用组)	可转换为通用组(只要该组不隶属于任何一个全局组)	可转换为通用组(只要该组不包含本地域组)

5.8.3 在单个域中使用组的策略

当在单个域中使用组时,可以使用 AGDLP 策略。AGDLP 策略:指把用户账户(A)放入全局组(G),再把全局放入本地域组(DL),然后给本地域组授予权限(P)。

当设置组时,使用以下策略。

(1) 把具有相同职责或有相同网络访问要求的用户账户添加到某个全局组。例如,管理员可以把所有访问相同资源的、负责市场业务的员工的用户账户添加到名为“G_市场部”的全局组中。

(2) 考虑是否使用内置的本地域组,必要的话要创建一个新的本地域组。例如,可以创建一个名为 DL_Color Printer Users 的本地域组,让用户能够使用域中共享的彩色打印机。

(3) 把所有有相同资源访问需求的全局组添加到本地域组里。例如,把创建的全局

组,包括 G_Sales,添加到本地域组 DL_Color Printer Users 中。

(4) 授予本地域组访问资源的必需权限,例如,授予本地域组 DL_Color Printer Users 使用彩色打印机的必需权限。

5.8.4 创建与管理域组

1. 域组的新建、重命名、删除

要在域 xyz.net 中的"市场部"OU 中,新建一个名为"G_市场部"的安全式全局组,操作步骤为:打开"Active Directory 用户和计算机"→单击域名(xyz.net)→右击"市场部"OU→"新建"→"组",在弹出的对话框中输入组名(G_市场部)、供早期操作系统(例如 Windows NT)访问的组名、选择组的作用域(全局组)和类型(安全组),如图 5-28 所示。



图 5-28 新建域中的组

每个组都有一个唯一的、不能重用的安全标识符(SID)。Windows 2003 使用 SID 来识别该组,权限的设置也是通过 SID 设置的,而不是利用组名称。

域组的重命名:右击组账户→选择"重命名"→输入新的组账户名称。更改组账户名称后,由于该组的安全识别码(SID)并没有改变,因此该组账户的属性、权利与权限设置都不会变化。

域组的删除:右击组账户→选择"删除"。当删除一个组账户后,如果又创建了一个相同名称的新组,系统会给新组分配一个新的 SID,也就是说,新组永远也不会使用已删除组的 SID。因此,不能通过创建一个相同名称的组来恢复访问资源的权限。当删除组时,与该组相关联的权限也被一并删除,但不会把它的成员(用户账户或组)删除。

2. 在域组中添加成员

创建一个组之后,可以向该组中添加成员。组的成员可以是用户账户、其他的组或计算机账户。

要添加组的成员,操作步骤为:打开"Active Directory 用户和计算机"→展开域→展

开容器或组织单位→右击组→选择“属性”→选择“成员”选项卡→单击“添加”→单击“高级”→单击“立即查找”→选择要加入的成员(按 Shift 键或 Ctrl 键可以同时选择多个账户)→单击“确定”按钮,如图 5-29 所示。



图 5-29　在域组中添加成员

第6章 组 策 略

学习目标

学习完本章后，了解组策略的概念、功能以及组策略的结构。掌握使用组策略管理单元的方法，能够配置计算机和用户的组策略设置，并能够应用组策略，实现预期的管理目的。掌握创建组策略对象、链接现有组策略对象的方法。理解组策略继承的规则以及如何控制组策略的处理过程。

6.1 组策略概述

组策略为管理员提供了集中管理网络中的用户和计算机的方法。可以将组策略应用于整个网络，也可以只应用于指定的用户和计算机。通过使用组策略，可以定义用户初始的工作环境状态，然后可以根据实际需求不断改进已定义的组策略设置。组策略的应用，可以降低配置用户环境的复杂性，减少用户错误配置环境的可能性，减少网络管理员技术支持的工作量，使得管理用户和计算机的工作变得更加灵活、方便，从而提高工作效率。

6.1.1 组策略功能

组策略可以实现以下功能。

(1) 在站点或域上，实施应用于整个企业的集中化的策略；在组织单位(OU)级别上，实施应用于每个部门的分散化的策略。

(2) 确保用户能在满足工作需要的环境中工作。例如，可以自动安装软件；用户的数据文件能有一个集中、安全的存储位置等。

(3) 控制用户和计算机的环境，从而可以减少用户所需的技术支持。例如，通过使用组策略，能够防止用户随意更改系统配置，还能防止用户安装不必要的应用程序。

(4) 实施公司策略，包括商业规范、目标和安全要求。例如，确保所有用户的安全配置都符合公司的安全要求，确保所有用户都已经安装了一组特定的应用程序集合。

6.1.2 组策略对象

组策略的设置包含在组策略对象(Group Policy Object，GPO)中，因此，只要将GPO关联到指定的站点、域或OU，该GPO内的设置就会影响该站点、域或OU内的所有用户与计算机。

GPO有两种类型：本地GPO和非本地GPO。

运行Windows 2003的计算机不论是在工作组环境中，还是在Active Directory环境

中，在本机上都存储了一个本地 GPO。然而，如果一台计算机已经加入 Active Directory 域，那么非本地 GPO 就能覆盖本地 GPO。在工作组环境中或者在未联网的环境中，由于本地 GPO 的设置并没有被非本地 GPO 覆盖，所以本地 GPO 有效。

非本地 GPO 是与 Active Directory 对象(例如站点、域或组织单位)关联起来使用的，非本地 GPO 也可以应用于用户或计算机。如果要使用非本地 GPO，网络中必须有一台 Windows 2003 域控制器，并且系统会分层次应用非本地 GPO 中的策略，从计算机所在的站点到计算机所在的组织单位，并且这些组策略的应用是累加的。如果没有特别说明，本书中所指的都是非本地 GPO。

Windows 2003 域控制器内已经有两个内建 GPO，分别如下。

(1) Default Domain Policy。该 GPO 已被链接到域，因此它的设置会被应用到整个域内的所有用户与计算机。

(2) Default Domain Controllers Policy。该 GPO 已被链接到 Domain Controllers OU，因此它的设置会被应用到域控制器组织单位内的所有用户与计算机。在域控制器组织单位内，系统默认只有域控制器的计算机账户。

打开“Active Directory 用户和计算机”，右击 Domain Controllers OU→“属性”→“组策略”，可以看到 Default Domain Controllers Policy 这个 GPO 已经被链接到 Domain Controllers OU 上，如图 6-1 所示。

打开“Active Directory 用户和计算机”，右击域名称→“属性”→“组策略”，可以看到 Default Domain Policy 这个 GPO 已经被链接到整个域，如图 6-2 所示。




图 6-1 Default Domain Controllers Policy



图 6-2 Default Domain Policy

提示：请勿随意修改 Default Domain Policy 或 Default Domain Controllr Policy 的 GPO 配置，以免操作系统不正常运行。

除了可以针对站点、域与组织单位来设置组策略之外，还可以针对每一台计算机配置本地计算机策略，本地计算机策略的配置数据是被存储在本地计算机的%systemroot%

System32\GroupPolicy 文件夹内，它是一个隐藏文件夹。本地计算机策略只会应用到本地计算机以及在此计算机登录的所有用户。

6.1.3 使用组策略管理单元

组策略管理单元的根节点显示为 GPO 名称及所属的域，格式如下：

GPO 名称 [域名]策略

例如，Default Domain Controllers Policy [server01. xyz. net]策略，如图 6-3 所示。



图 6-3 Default Domain Controllers Policy 管理单元

1. “本地计算机”策略管理单元

每台运行 Windows 2003 的计算机上都可以设置本地计算机策略。要打开“本地计算机”策略管理单元，操作步骤为：单击“开始”→“运行”，在“打开”中输入 mmc，单击“确定”按钮，启动 MMC，单击 MMC 的“文件”菜单，选中“添加/删除管理单元”，打开“添加/删除管理单元”对话框，单击“独立”选项卡内的“添加”按钮，打开“添加独立管理单元”对话框，向下滚动“可用的独立管理单元”列表，选中“组策略对象编辑器”，单击“添加”按钮，打开选择“组策略对象”对话框，确保“本地计算机”出现在“组策略对象”框中，单击“完成”按钮，单击“关闭”按钮，关闭“添加独立管理单元”对话框，单击“确定”按钮，关闭“添加/删除管理单元”对话框。如图 6-4 所示，“本地计算机”策略管理单元已经添加到了 MMC 控制台中。

提示：在如图 6-5 所示的对话框中，单击“浏览”按钮，将弹出“浏览组策略对象”对话框，可选择网络中的任何域、组织单位、站点或计算机(这台计算机或另一台计算机)的组

策略对象。

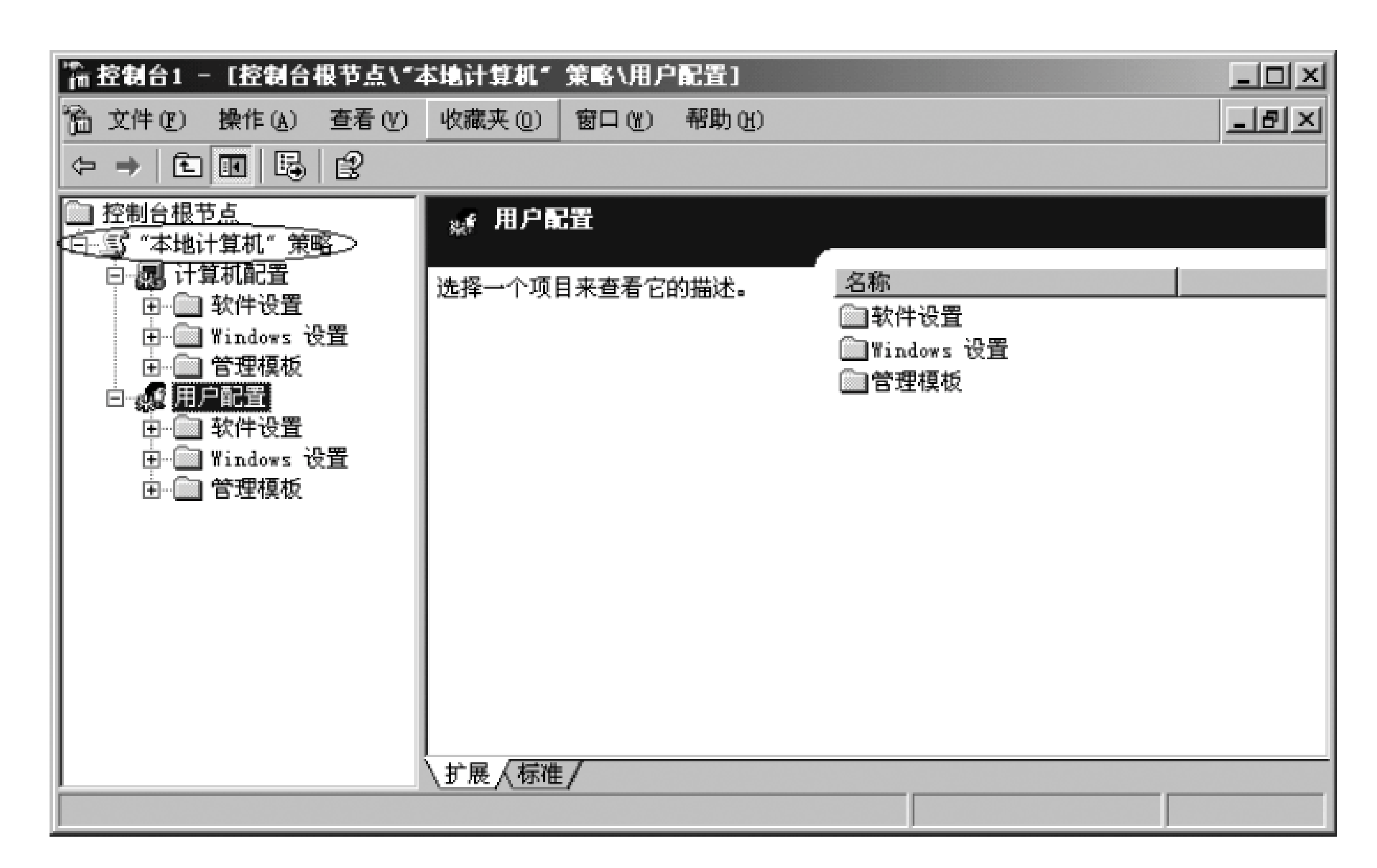


图 6-4　本地计算机策略



图 6-5　组策略向导

2. 在"Active Directory 用户和计算机"中打开组策略管理单元

利用"Active Directory 用户和计算机"管理单元，可以为 Active Directory 对象(例如域、组织单位和站点)创建新的 GPO 或编辑已有的 GPO。操作步骤为：打开"Active Directory 用户和计算机"管理单元，右击要设置组策略的域或组织单位→"属性"，单击"组策略"选项卡，在"组策略对象链接"列表中，单击"新建"创建一个新的 GPO，然后单击"编辑"。或者选中一个已有的 GPO，然后单击"编辑"，从而启动所选域或组织单位的组策略管理单元。

3. 在“Active Directory 站点和服务”中打开组策略管理单元

利用“Active Directory 站点和服务”管理单元，可以为 Active Directory 站点创建新的 GPO 或编辑已有的 GPO。操作步骤为：打开“Active Directory 站点和服务”管理单元，右击要设置组策略的站点→“属性”，单击“组策略”选项卡，在“组策略对象链接”列表中，单击“新建”创建一个新的 GPO，然后单击“编辑”。或者选中一个已有的 GPO，然后单击“编辑”，从而启动选中站点的组策略管理单元。

提示：微软公司还另外提供了一个名为 Microsoft Group Policy Management Console（GPMC）的管理工具，使管理员能够更容易地管理组策略。

6.1.4 配置计算机和用户的组策略

GPO 中包含两个不同的节点：“计算机配置”和“用户配置”。

（1）计算机配置。定义的设置有操作系统设置、桌面设置、安全设置、启动/关机脚本的设置，已分派的应用程序选项以及应用程序设置。在操作系统初始化以及系统刷新时，将应用与计算机相关的组策略。一般来说，在计算机的组策略与用户的组策略发生冲突时，将优先应用计算机的组策略。

（2）用户配置。定义的设置有操作系统设置、桌面设置、安全设置、已分派和已发行的应用程序选项、应用程序设置、文件夹重定向选项以及登录/注销脚本。在用户登录到计算机以及在系统刷新时，将应用与用户相关的组策略。

通过编辑 GPO 可以配置组策略设置，从而定义影响用户和计算机的策略。可以配置的组策略设置的类型如下。

（1）管理模板。用于配置应用程序以及用户桌面环境的基于注册表的设置。这些设置包括用户能够访问的操作系统组件和应用程序，用户对“控制面板”的访问级别以及用户对脱机文件的控制级别。

（2）安全设置。用于配置本地计算机、域和网络安全性的设置。这些设置包括对用户访问网络的控制、对账户和审核策略的设置以及对用户权限的控制。

（3）软件安装。为用户提供一个可以获得应用程序的集中位置，在客户端计算机自动进行应用程序的安装、更新或删除。

（4）脚本。指定在计算机启动/关闭、用户登录/注销时运行脚本，可以指定某些脚本执行批处理操作、控制多个脚本以及指定脚本的运行顺序。

（5）远程安装服务。控制用户在使用“远程安装服务”运行“客户安装向导”时的可用选项。

（6）Internet Explorer 维护。管理和自定义 Internet Explorer 的设置。

（7）文件夹重定向。用于将用户的文件夹（例如“我的文档”文件夹）重定向到网络服务器上的一个共享文件夹内。

6.1.5 应用组策略的时间

当修改了站点、域或 OU 的 GPO 配置后，这些配置并不是立即就应用到站点、域或 OU 内的用户与计算机。应用 GPO 配置的具体时间与修改的是计算机配置还是用户配置有关。

1. 计算机配置的启用时间

(1) 计算机开机时自动启用。

(2) 即使计算机不重新开机，系统仍然会每隔一段时间自动启用。域控制器默认每隔 5min 自动启用，非域控制器默认每隔 90～120min 自动启用，而且无论策略配置值是否有变动，系统仍然会每隔 16h 自动启用一次。

(3) 手动启用。在命令提示符中执行 gpupdate/target：computer /force 命令。

2. 用户配置的启用时间

(1) 用户登录时自动启用。

(2) 即使用户不注销、登录，系统仍默认每隔 90～120min 自动启用，而且不论策略配置值是否有变动，系统仍然会每隔 16h 自动启用一次。

(3) 手动启用。在命令提示符中执行 gpupdate/target：user/force 命令。

提示：打开“事件查看器”中的“应用程序”日志，双击来源为 SceCli 的事件，检查组策略是否已经启用成功。部分的组策略配置，必须等待计算机重新启动或用户登录时才有效，例如“软件安装策略”与“文件夹重定向策略”等。

6.2 使用组策略对象

如果现有的 GPO 设置已经可以满足需求，那么就可以把该 GPO 直接链接到站点、域或组织单位。如果要创建新的 GPO 或者编辑现有的 GPO 时，默认的操作是对域控制器上的 GPO 进行管理，而这些域控制器必须是主域控制器(PDC)模拟器的角色。

6.2.1 创建组策略对象

可以创建有链接的 GPO，也可以创建无链接的 GPO。要创建链接到站点、域或组织单位的 GPO 时，要先创建一个新的 GPO，然后将其链接到站点、域或组织单位，需满足以下条件。

(1) 必须具有对与 GPO 相链接的站点、域或组织单位的 gPLink 和 gPOptions 两个属性的“读取”和“写入”权限。

(2) 默认情况下，只有 Domain Admins 和 Enterprise Admins 组的成员才拥有将 GPO 链接到域和组织单位的必要权限，只有 Enterprise Admins 组的成员才拥有将 GPO

链接到站点的必要权限。

(3) Group Policy Creator Owners 组的成员能够创建 GPO,但不能将其链接到站点、域或组织单位。

1. 创建有链接的组策略对象

要为域或组织单位创建有链接的 GPO,操作步骤为:打开"Active Directory 用户和计算机",右击要为其创建 GPO 的域或组织单位→"属性"→"组策略"选项卡,单击"新建",输入新建 GPO 的名称,然后按 Enter 键。新建的 GPO 会出现在"组策略"选项卡中的 GPO 列表内,这样该列表中的 GPO(包括新建的 GPO)就链接到了与该选项卡所对应的组织单位或域上了。

提示:利用"Active Directory 站点和服务"管理单元可创建链接到站点的 GPO,只有 Enterprise Admins 组的成员,才能创建链接到站点的 GPO。

2. 创建无链接的组策略对象

在实际环境中,可能会由一个组负责创建 GPO,而由另外一个组负责把创建的 GPO 链接到所需的站点、域或组织单位。

要创建无链接的 GPO,操作步骤为:单击"开始"→"运行",在"打开"中输入 mmc,单击"确定"按钮,启动 MMC,单击 MMC 的"文件"菜单,选中"添加/删除管理单元",打开"添加/删除管理单元"对话框,单击"独立"选项卡内的"添加"按钮,打开"添加独立管理单元"对话框,向下滚动"可用的独立管理单元"列表,选中"组策略对象编辑器",单击"添加",打开选择"组策略对象"对话框,在选择"组策略对象"对话框中,单击"浏览"按钮,在"浏览组策略对象"对话框中,单击"全部"选项卡,在"存储在本域中的所有组策略对象"列表中右击,单击"新建"→输入新建 GPO 的名称,按 Enter 键确认,单击"确定"按钮,关闭"浏览组策略对象"对话框。

要编辑新建的 GPO,可以在选择"组策略对象"对话框中单击"完成"按钮,然后在控制台树中编辑新建的 GPO。

6.2.2 链接现有组策略对象

1. 将现有 GPO 链接到域和组织单位

要将现有 GPO 链接到域和组织单位,操作步骤为:打开"Active Directory 用户和计算机",右击要与现有 GPO 相链接的域或组织单位→"属性"→"组策略"选项卡,单击"添加"按钮,单击"添加组策略对象链接"对话框中的选项卡(例如域/OUs、站点或全部),在"查找范围"下拉框中,选择要与之链接的 GPO 所在的域,在组策略对象列表中,选择要与之链接的 GPO,单击"确定"按钮。

2. 将现有 GPO 链接到站点

利用"Active Directory 站点和服务"管理单元,任何 Enterprise Admins 组的成员都

能够将现有 GPO 链接到站点上。默认情况下，只有 Enterprise Admins 组的成员才能够将现有的 GPO 链接到站点上。但是任何一个对这个现有的 GPO 具有“读取”和“写入”权限的用户都能对它进行更改，一旦这个被更改的 GPO 被链接到了站点上，该 GPO 将会影响整个站点，可能会造成严重的后果。因此最好为站点创建新的 GPO，而不是将现有 GPO 链接到站点上。

6.3 组策略的处理规则

应用到用户或计算机的组策略设置是根据许多规则确定的。只有充分理解了这些规则，才能灵活地管理用户与计算机的环境，达到预期的管理效果。

组策略的继承与处理规则，也就是应用组策略的顺序，将决定哪些组策略设置最终会影响用户和计算机。

1. 一般的继承与处理规则

一般的继承与处理规则如下。

(1) 如果父容器配置了组策略，但其子容器未配置组策略，则子容器将继承父容器配置的组策略。

(2) 如果子容器配置了组策略，则此配置会覆盖由其父容器所传递下来的组策略配置。

(3) 组策略的配置具有累加性。例如，如果在“市场部”OU 内建立了 GPO，同时在域、站点内都有 GPO，则域、站点与 OU 内的所有 GPO 配置值都将被累加起来作为“市场部”OU 最后有效的组策略配置。

(4) 处理 GPO 的先后顺序是：站点的 GPO→域的 GPO→OU 的 GPO。当域、站点与 OU 之间的 GPO 配置发生冲突时，则以处理顺序在后的 GPO 优先，因此 OU 的 GPO 配置优先。

(5) 先处理“计算机配置”，再处理“用户配置”。如果“计算机配置”与“用户配置”发生冲突，大多情况下却是以“计算机配置”优先。

(6) 如果将多个 GPO 链接到同一个 OU，那么所有 GPO 的配置将被累加起来，作为这个 OU 最后有效的组策略配置，如果这些 GPO 的配置发生冲突，则将排在 GPO 列表顶端的 GPO 配置优先。

(7) 在域环境中，“本地计算机策略”内的组策略配置如果与站点、域或 OU 的组策略配置发生冲突，则站点、域或 OU 的配置优先，“本地计算机策略”的配置无效。

2. 例外的组策略处理规则

除了一般的继承与处理规则外，还可以配置以下例外规则。

(1) 阻止策略继承。通过选择子容器内“阻止策略继承”选项来设置子容器不继承由父容器传递来的所有 GPO 配置，也就是只以子容器的 GPO 作为组策略的配置。如果子容器的 GPO 内设置为“尚未配置”，则采用默认值。

(2) 禁止替代。选择父容器中的GPO链接(例如公司安全策略),单击“选项”,在链接选项中,选中“禁止替代”选项,可以强制子容器必须继承此GPO内的组策略设置,而不论子容器是否设置了“阻止策略继承”。如图6-6所示,设置在xyz.net域上的“公司安全策略”,此策略将会强制应用到域内的所有用户、计算机上。“禁止替代”的优先级高于“阻止策略继承”的优先级,因此“禁止替代”能使所有的组策略设置都能得到应用。“禁止替代”选项是设置在链接上的,而不是在GPO上。如果某GPO链接到多个容器,那么可以互相独立地为每个容器设置“禁止替代”选项。

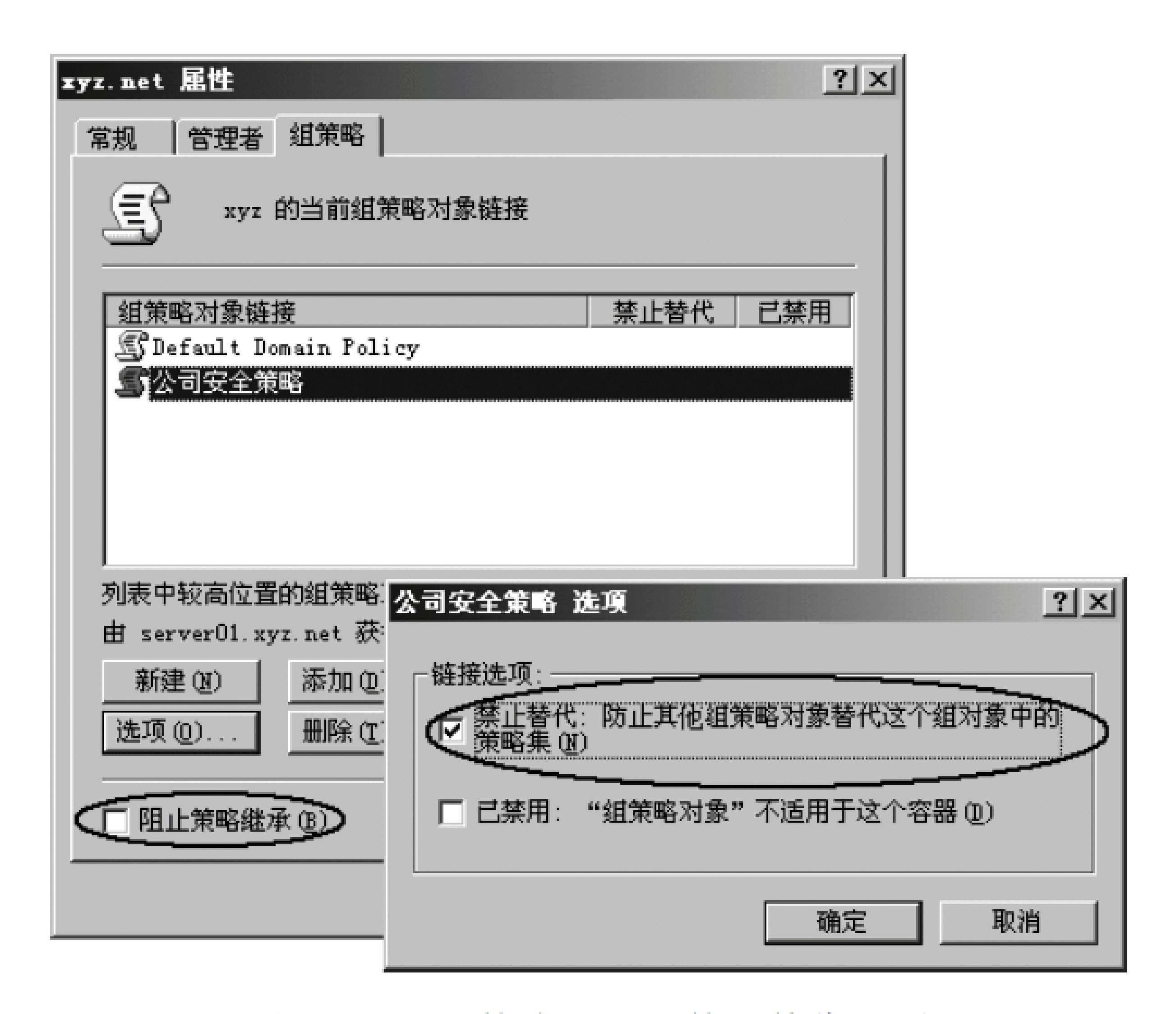


图6-6 阻止策略继承和禁止替代选项

(3) 组策略筛选

默认情况下,位于容器内的所有用户与计算机,默认对该容器的GPO都具有“读取”与“应用组策略”权限,因此,在某个容器上建立GPO后,此GPO的设置将被应用到这个容器内的所有用户与计算机。组策略筛选可以设置此GPO不应用到特定的用户、组或计算机对象。

例如,“市场部”OU的GPO配置可以限制所有市场部员工的工作环境,通过组策略筛选设置,可以不限制市场部内用户“王武”的工作环境。

要实现组策略筛选,操作步骤为:选择“市场部”OU的GPO链接→“属性”→“安全”选项卡,Authenticated Users表示所有经过身份验证的用户与计算机,其默认的权限为允许读取和应用组策略。若不想将此GPO的设置应用到此容器内的用户wangwu,则只需单击“添加”按钮,添加用户wangwu,然后“拒绝”wangwu的这两个权限即可,如图6-7所示。

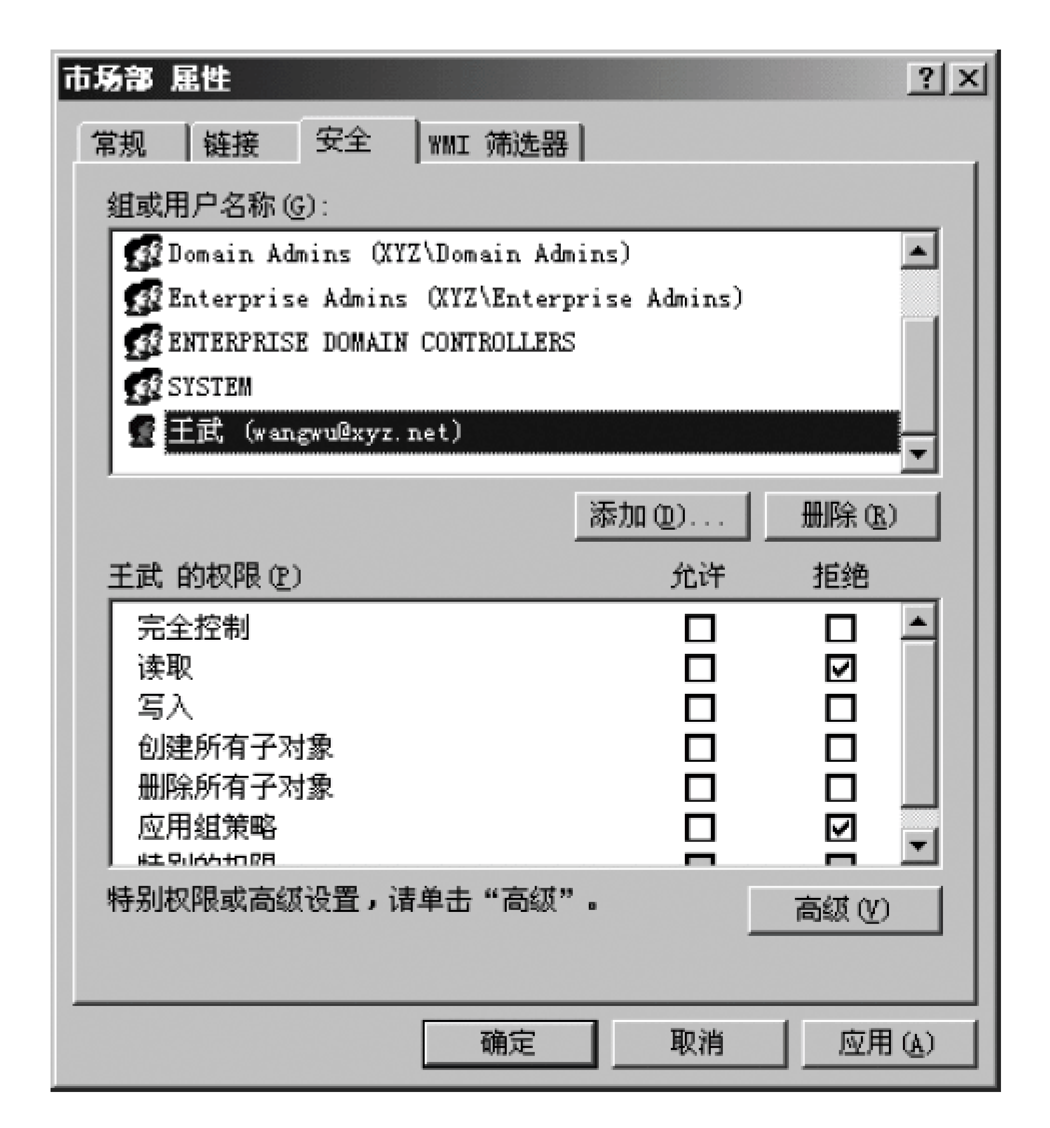


图 6-7　实现组策略筛选

6.4　计算机安全策略

网络管理员必须采取各种安全措施来确保用户的计算机环境和系统服务的安全。使用组策略中的安全设置策略，可以防止用户破坏计算机的各种设置，保障用户环境和网络的安全。

实现安全策略最有效的方式是使用安全模板，安全模板是一系列安全设置的集合，并可根据组织需要，调整安全模板的设置。使用安全模板可以简化定义和实现一组标准的组策略的过程。利用 Windows 2003 提供的安全配置和分析工具，可以对用户和计算机的安全策略进行分析和配置。

Windows Server 2003 还提供了审核功能，管理员可以通过分析安全日志文件查看资源的被访问情况。

实施安全策略可以设置每台计算机的本地安全策略来配置单台计算机，也可以设置域中的组策略来配置多台计算机。使用何种方式取决于公司的规模及其安全需求。在较小规模的或不使用 Active Directory 服务的网络中，可为每台计算机配置本地安全设置策略，这些安全策略仅影响本地计算机。在使用 Active Directory 服务的较大规模的网络中，可以在域、组织单位层次上应用安全策略，确保提供高级别的安全性。

域安全策略会影响域中的工作站和成员服务器。组织单位安全策略会影响该组织单位内的所有用户和计算机等对象。域控制器安全策略就是在 Active Directory 的 Domain Controllers 组织单位上实施的安全策略。

以本地安全策略、域安全策略和域控制器安全策略为例，介绍安全策略的设置方法。

1. 本地安全策略的设置

在非域控制器的计算机上，单击“开始”→“管理工具”→“本地安全策略”→打开“本地安全设置”管理单元，如图 6-8 所示。安全策略主要包括账户策略和本地策略。



图 6-8 本地安全设置

1）账户策略的设置

在账户策略中，可以配置密码策略和账户锁定策略，用于减少未经授权的用户访问网络的可能性。

展开“安全设置”→“账户策略”→“密码策略”，可以设置与账户密码有关的策略，如图 6-9 所示。

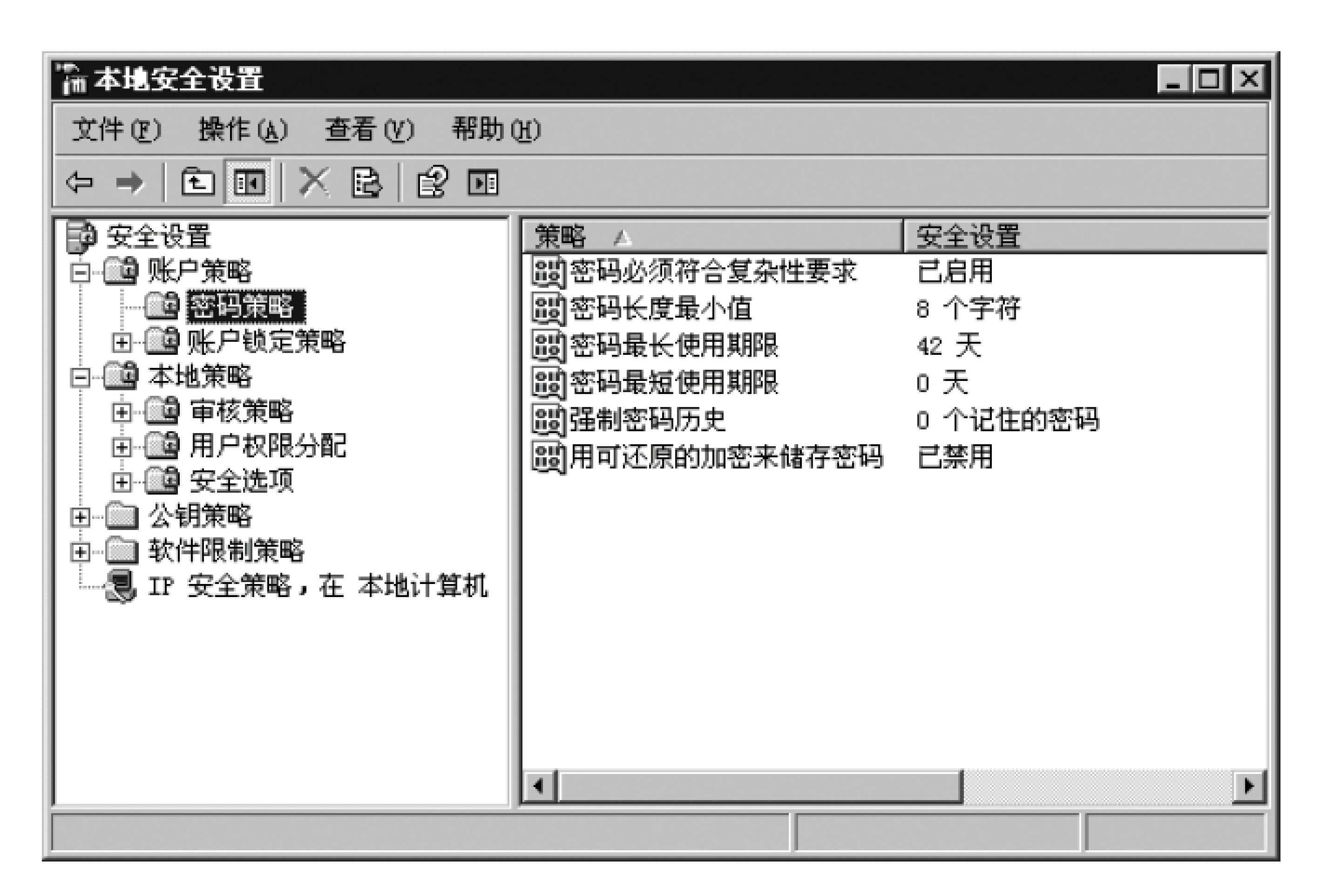


图 6-9 密码策略

(1) 密码必须符合复杂性要求。如果启用该项，则密码必须满足：不可以包含用户账户名称的全部或部分文字；至少要 6 个字符；至少要包含 A～Z、a～z、0～9、非字母数字

(例如!、¥、#、%)等4组字符中的3组。

(2) 密码最长使用期限。用来设置密码最长的使用期限。如果密码的使用期限已到,则用户在登录时系统会要求用户更改密码。如果设为0,表示密码没有使用期限,可以一直使用。默认值是42天。

(3) 密码最短使用期限。用来设置密码最短的使用期限,在未到期前,用户不得更改密码。如果设为0,则表示用户可以随时更改密码。默认值是0。

(4) 强制密码历史。用来记录用户使用密码的历史。在用户设置新密码时,以便决定是否允许用户使用曾经使用过的旧密码。此处的值可为0~24,默认值是0。1~24表示要保存密码历史记录。例如,如果设为6,则用户的新密码不能与前6次使用过的旧密码相同。0表示不保存密码历史记录。密码可以重复使用,也就是用户在更改密码时,可以使用以前使用过的旧密码。

(5) 密码长度最小值。用来设置用户的密码至少需要几个字符。此处的值可为0~14,如果设为0,则表示可以没有密码。默认值是0。

(6) 用可还原的加密来存储密码。此项为某些应用程序提供支持,这些应用程序使用的协议需要用户密码来进行身份验证。使用可还原的加密储存密码与储存纯文本密码在本质上是相同的。因此,除非应用程序需求比保护密码信息更重要,否则绝不要启用此策略。

展开"安全设置"→"账户策略"→"账户锁定策略",可以设置与账户锁定相关的策略,如图6-10所示。

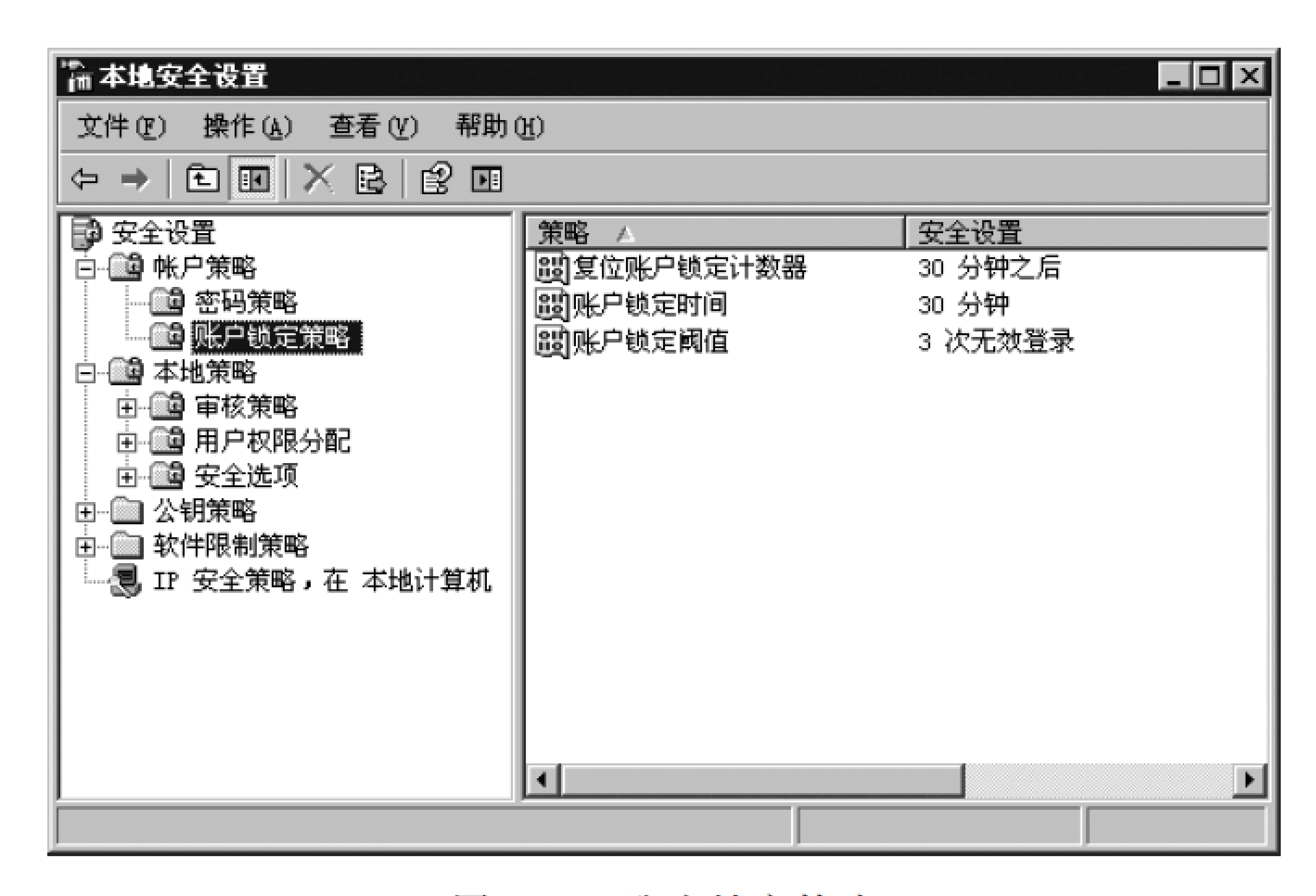


图6-10 账户锁定策略

(1) 账户锁定阈值。用来设置用户登录失败超过一定的次数后,就将该用户账户锁定。在解除锁定之前,用户无法再利用该账户登录。此处的值为0~999,如果设为0,则表示账户永远不会被锁定。默认值是0。

(2) 账户锁定时间。用来设置锁定账户的持续时间,过了这段时间之后就自动解除锁定。此处的值为0~99999min,如果设为0min,则表示该账户将被永久锁定,不会自动解除锁定,除非系统管理员手工解除锁定,也就是将用户账户属性中的"账户已锁定"选项

清除。

(3) 复位账户锁定计数器。“锁定计数器”是用来记录用户登录失败的次数,初始值为0,如果用户登录失败,则锁定计数器的值就会增加1。如果登录成功,则锁定计数器的值就会归0。如果锁定计数器的值等于账户锁定阈值,该账户就会被锁定。可以设置登录失败的时间间隔,以便使锁定计数器的值在间隔时间到后自动归0。

以图6-11中的设置为例进行说明,如果用户连续3次登录失败,其账户就会被锁定。但是在被锁定之前(尚未连续3次登录失败),如果前一次登录失败后到这一次失败之间的间隔时间已经超过30min,则锁定计数器的值就会从0开始计算,也就是这次登录失败仍然算是第1次。

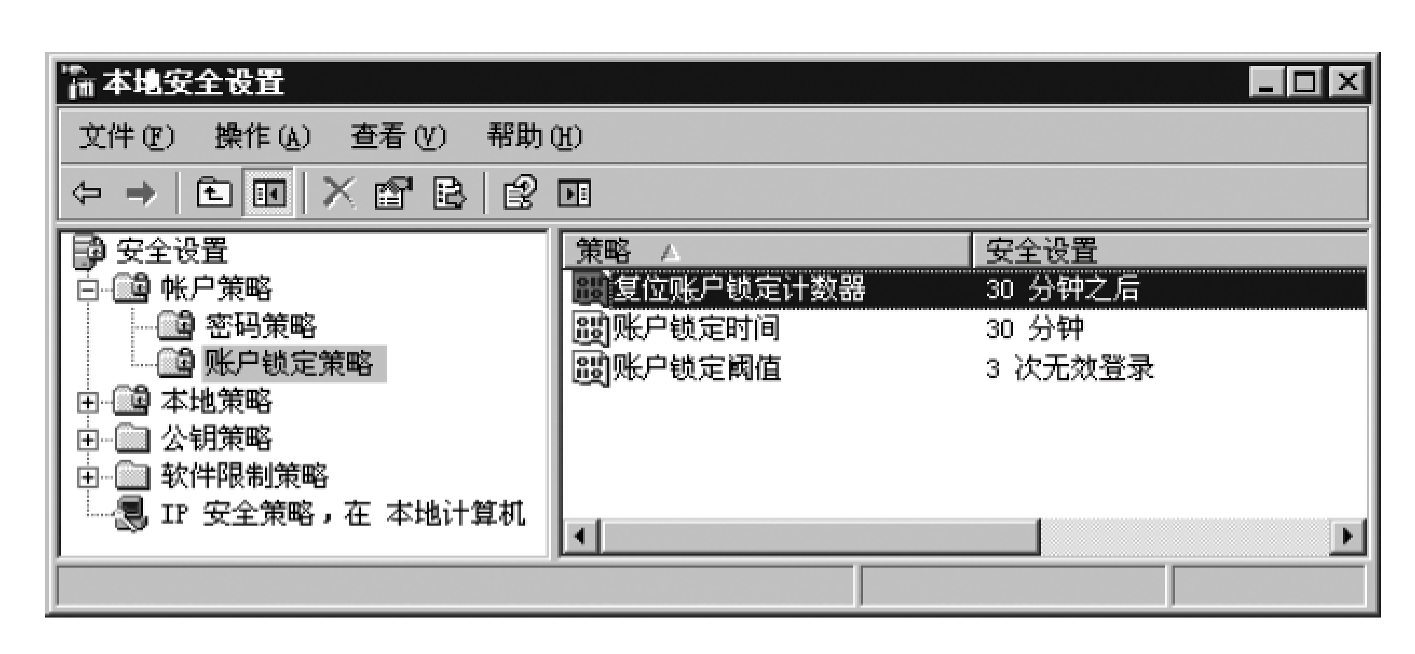


图6-11 账户锁定策略的设置

2) 本地策略

本地策略包含“审核策略”、“用户权限分配”与“安全选项”。关于“审核策略”,在后面的章节中介绍,在此仅介绍后两项。

展开“安全设置”→“本地策略”→“用户权限分配”,可以将执行特殊任务的权限分配给用户或组,如图6-12所示。



图6-12 用户权限分配

要将执行特殊任务的权限分配给用户或组，双击某策略项或右击某策略项设置其属性。假设要给某用户或组分配“从远程系统强制关机”的权限，在出现图 6-13 时，单击“添加用户或组”按钮，添加要授予该权限的用户或组即可。

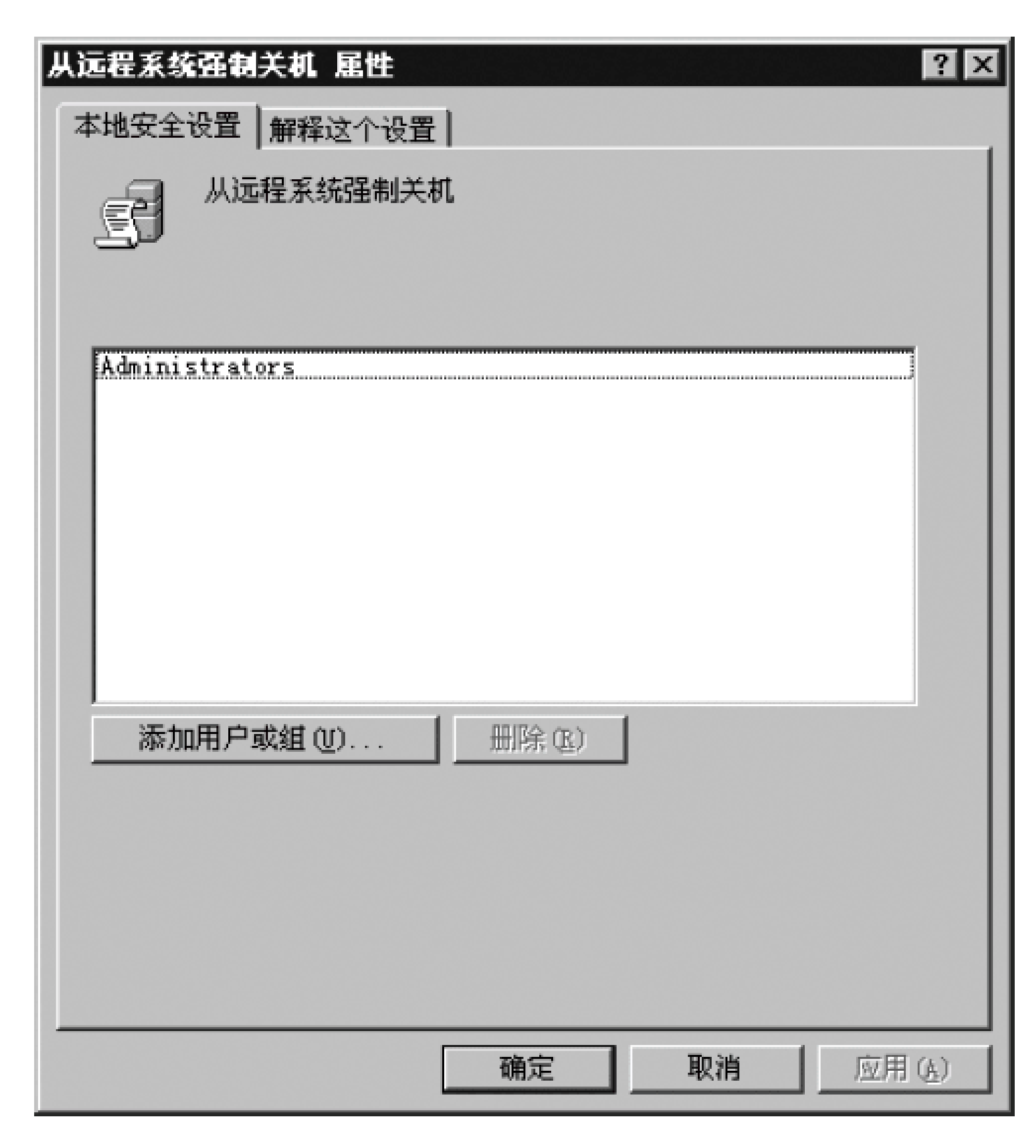


图 6-13　从远程系统强制关机策略设置

下面仅介绍常见的用户权限策略。

(1) 允许在本地登录。允许用户在本地计算机上登录。

(2) 拒绝本地登录。拒绝用户在本地计算机上登录，此权限优先于“允许在本地登录”的权限。

(3) 域中添加工作站。允许用户将客户端计算机加入域。

(4) 关闭系统。允许用户关闭计算机。

(5) 从网络访问此计算机。允许用户通过网络上的其他计算机访问该计算机内的资源。

(6) 拒绝从网络访问此计算机。拒绝用户通过网络上的其他计算机来访问该计算机内的资源，此权限优先于“从网络访问此计算机”的权限。

(7) 从远程系统强制关机。允许用户从远程计算机关闭此计算机。

(8) 备份文件和目录。允许用户备份硬盘中的文件与文件夹。

(9) 还原文件和目录。允许用户还原所备份的文件与文件夹。

(10) 管理审核和安全日志。允许用户指定要审核的事件、查询与清除安全日志。

(11) 更改系统时间。允许用户更改计算机内部的系统日期、时间。

(12) 装载和卸载设备驱动程序。允许用户添加/删除硬件，管理设备的驱动程序。

(13) 取得文件或其他对象的所有权。允许用户取得其他用户拥有的文件、文件夹或对象的所有权。

展开“安全设置”→“本地策略”→“安全选项”，可以启用或禁用计算机的一些安全设

置，如图 6-14 所示。

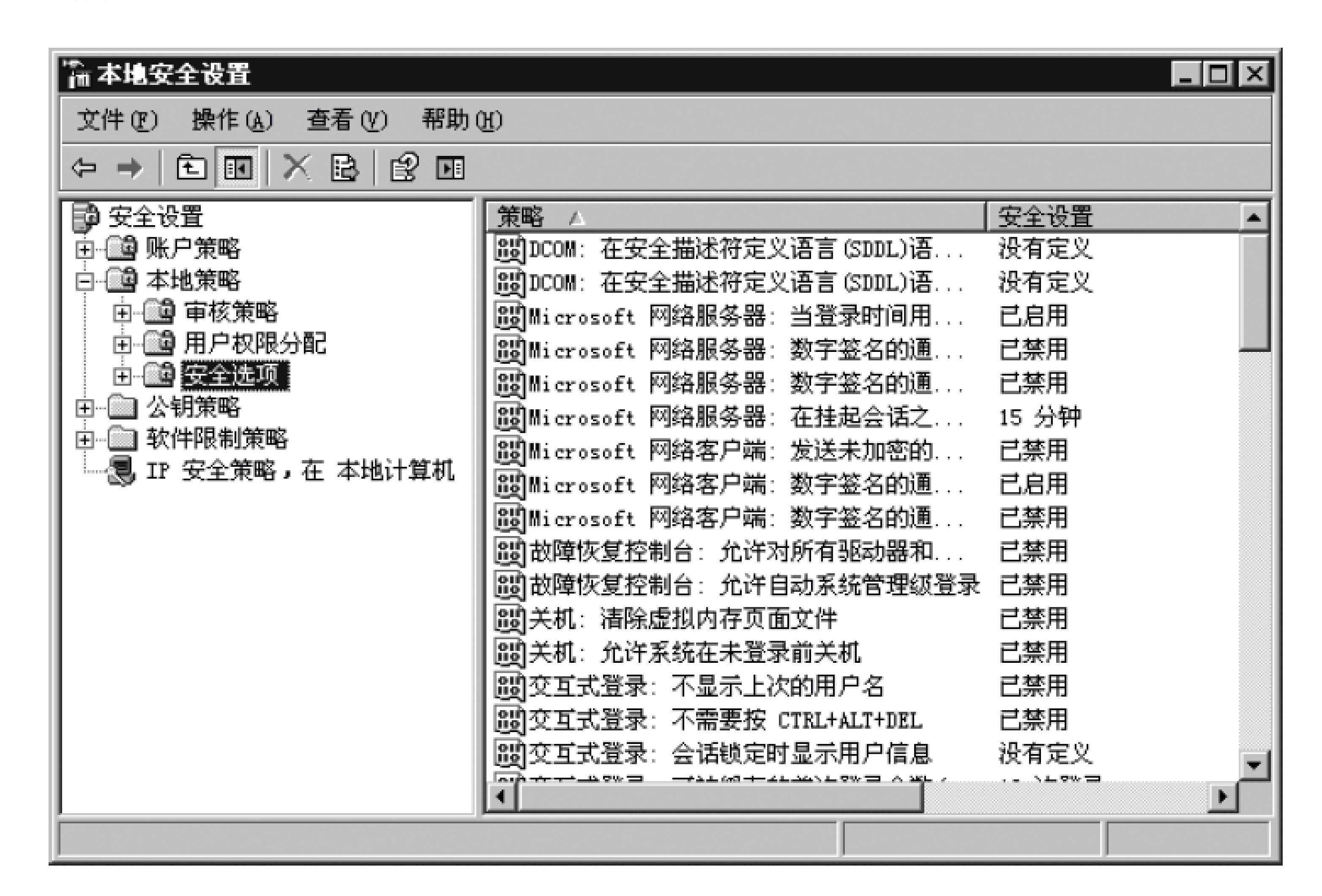


图 6-14　安全选项

下面仅介绍常见的安全选项。

(1) 关机：允许系统在未登录前关机。按 Ctrl＋Alt＋Delete 组合键后，单击“登录 Windows”窗口中的“关机”按钮，在未登录时就可以关闭计算机。

(2) 交互式登录：不需要按 Ctrl＋Alt＋Delete 组合键。计算机启动后直接出现“登录 Windows”的窗口，不显示“请按 Ctrl＋Alt＋Delete 组合键开始”的窗口。

(3) 交互式登录：不显示上次登录的用户名。按 Ctrl＋Alt＋Delete 组合键后，在出现的“登录 Windows”的窗口中不显示上一次登录的用户名。

(4) 交互式登录：在密码到期前提示用户更改密码。用来设置在用户的密码过期前，提前几天提示用户更改密码。

(5) 交互式登录：用户试图登录时消息标题/消息文字。系统每次启动时，都会显示“请按 Ctrl＋Alt＋Delete 组合键开始”的消息。如果需要在登录窗口中能自动显示一些消息，则可以分别利用这两项设置显示窗口的标题文字和显示窗口的文本。

(6) 账户：管理员账户状态。确定是启用还是禁用本地管理员账户，默认启用。

(7) 账户：来宾账户状态。确定是启用还是禁用来宾账户。默认禁用。

(8) 账户：使用空白密码的本地账户只允许进行控制台登录。设置使用空白密码的本地账户是否可以从物理计算机控制台之外的位置登录。默认启用。

(9) 账户：重命名来宾账户。来宾账户默认为 Guest，可重命名为其他名称。

(10) 账户：重命名系统管理员账户。来宾账户默认为 Administrator，可重命名为其他名称。重命名会使未授权的人猜测此用户名和密码组合的难度稍微大一些。

2. 域安全策略的设置

在域控制器上，单击“开始”→“管理工具”→“域安全策略”，打开“默认域安全设置”管

理单元,如图 6-15 所示。域安全策略会影响域中的工作站和成员服务器。

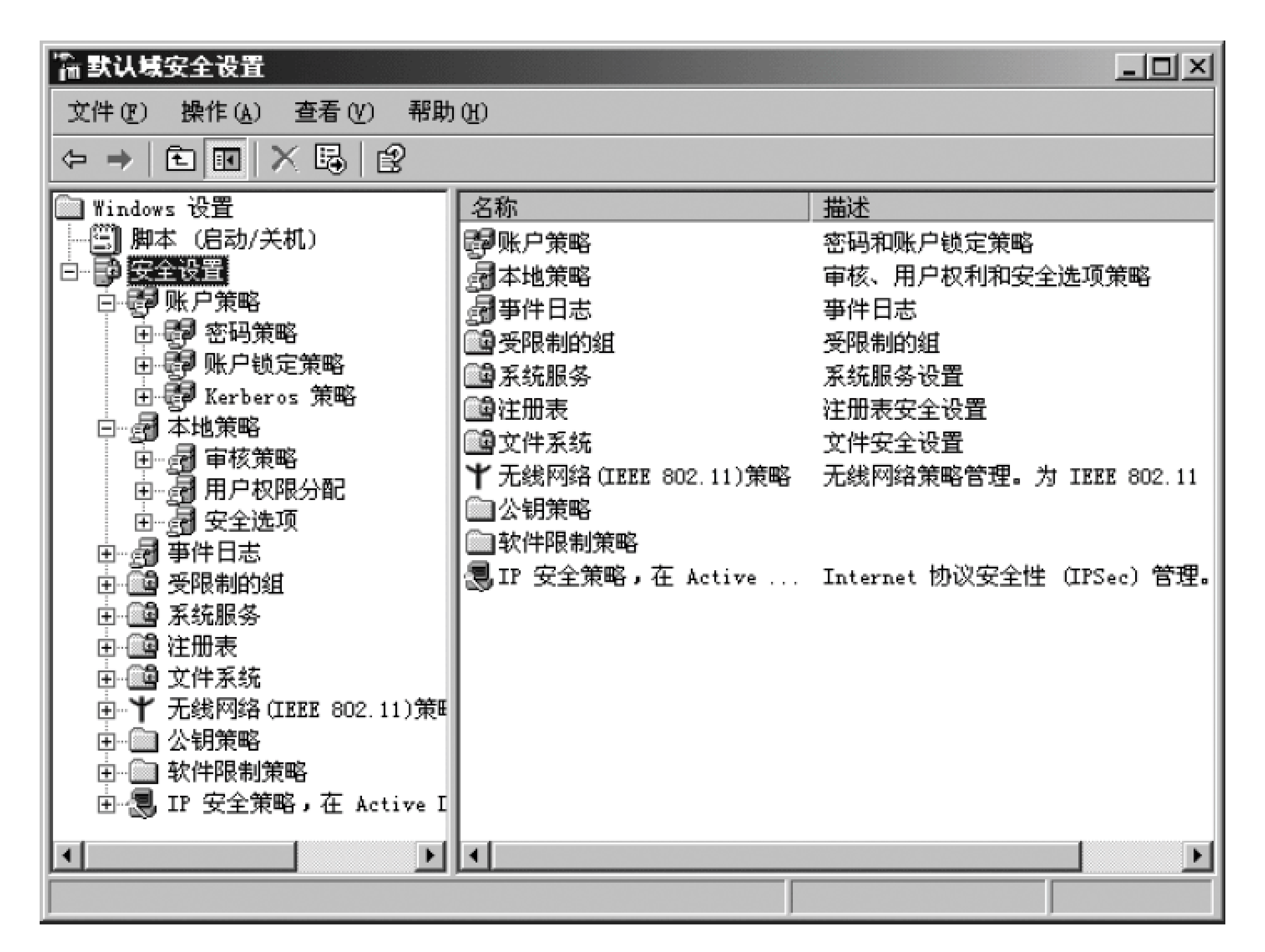


图 6-15 域安全策略的设置

域安全策略的设置与本地计算机策略的设置大致相同,需注意的事项如下。

(1) 域内的任何一台计算机,都会受域安全策略的影响。

(2) 域内的计算机,如果其"本地安全策略"的设置与"域安全策略"的设置发生冲突时,则以"域安全策略"的设置优先,"本地安全策略"的设置无效。只有在域安全策略的设置被设置成"没有定义"时,本地安全策略的设置才会有效。

(3) 修改"域安全策略"以后,应用修改后的域安全策略的时机如下。

① 安全策略有变化或计算机重新启动时。

② 域控制器每隔 5min 会自动应用;Windows Server 2003 成员服务器或 Windows XP Professional 每隔 90～120min 会自动应用。即使安全策略设置没有任何更改,所有计算机每隔 16h 也会自动强制应用域安全策略中的所有设置。

③ 执行 gpupdate /target:computer 命令手工刷新。如果要强制应用,请执行 gpupdate /target:computer /force 命令。

3. 域控制器安全策略的设置

组织单位的安全策略会影响该组织单位内的所有用户和计算机等对象。域控制器安全策略就是在活动目录的 Domain Controllers 组织单位上实施的安全策略,如图 6-16 所示。域控制器安全策略只会影响位于 Domain Controllers 组织单位内的对象,位于其他容器或组织单位内的计算机并不会受该策略的影响。

在域控制器上,单击"开始"→"管理工具"→"域控制器安全策略",打开"默认域控制器安全设置"管理单元,如图 6-17 所示。

"域控制器安全策略"的设置与"本地安全策略"、"域安全策略"的设置大致相同,需注

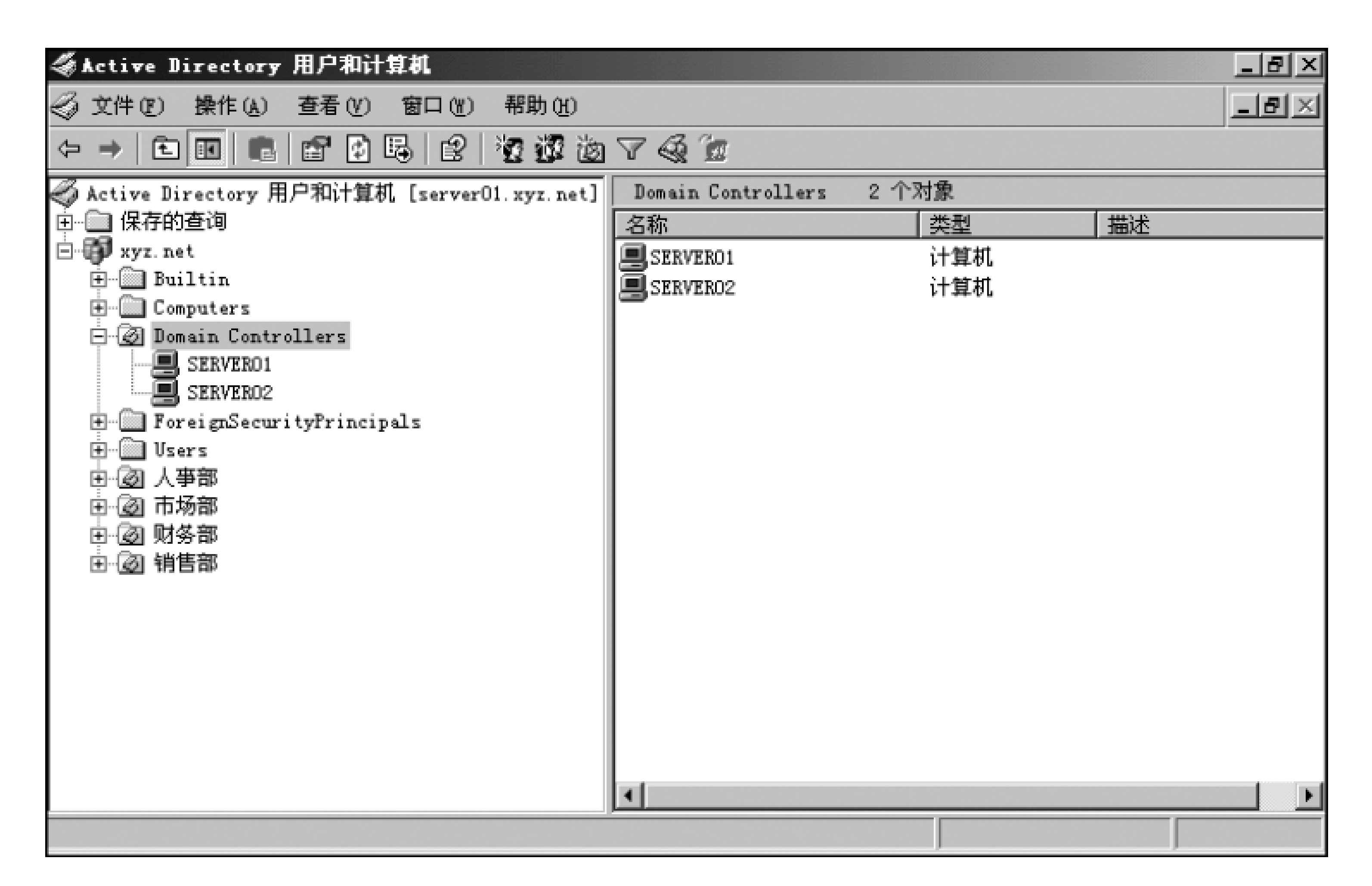


图 6-16 域控制器安全策略的设置



图 6-17 “默认域控制器安全设置”管理单元

意的事项如下。

(1) 位于 Domain Controllers 组织单位内的任何一台域控制器都会受“域控制器安全策略”的影响。

(2)“域控制器安全策略”与“域安全策略”的设置发生冲突时，对位于 Domain Controllers 组织单位内的对象来说，默认是“域控制器安全策略”的设置优先，即“域安全策略”的设置无效。例外的是，“域安全策略”中的“账户策略”设置会影响域内所有的用户，当然也包括位于 Domain Controllers 组织单位内的用户账户，此时“域控制器安全策略”中的“账户策略”设置对域控制器无效。

第 7 章　DNS 服务器

学习目标

学习完本章后，了解 NetBIOS 名称、主机名称的区别，重点了解主机名称的解析过程，掌握如何利用 DNS 服务器解析计算机名称，并能熟练掌握 DNS 服务器的安装、配置和维护。

7.1　名称解析概述

Windows Server 2003 通过计算机名与其他计算机通信时，实际上是要将计算机名解析为 32 位的 IP 地址，然后再利用 IP 地址和其他计算机通信。由计算机名解析为 IP 地址的过程称为“名称解析”。需要解析的计算机名称有两种类型：主机名称和 NetBIOS 名称。

主机名称最多可达 255 个字符，可以包含字母和数字、连字符和句号，可以追加计算机的域名，即完全限定域名（Fully Qualified Domain Name，FQDN）。要解析主机名称，可以利用 DNS 服务器进行动态解析，或者利用 HOSTS 文件（存储在%systemroot%\System32\Drivers\Etc 文件夹内）进行静态解析。

NetBIOS 名称共有 16 个字符，前 15 个字符是主机名称的前 15 个字符，第 16 个字符用来标识资源或在计算机上引用的服务。要解析 NetBIOS 名称，可以利用 WINS 服务器进行动态解析，或者利用 LMHOSTS 文件（存储在%systemroot%\System32\Drivers\Etc 文件夹内）进行静态解析。

在一个局域网中，一般使用 NetBIOS 名称即可区分不同的主机。而在 Internet 中一般借助主机名称区分不同的主机。主机名称最多可达 255 个字符，可以包含字母和数字、连字符和句号，可以追加计算机的域名，构成完全限定域名（FQDN）。可以利用 DNS 服务器进行动态解析或利用 HOSTS 文件（存储在%systemroot%\System32\Drivers\Etc 文件夹内）进行静态解析。

在 DNS 服务器的区域中，可以针对同一台主机建立不同的主机名称。例如，在一台 IP 地址为 192.168.10.1 的服务器上既做 Web 服务，又做 FTP 服务，这时可以在 xyz.net 区域中分别建立 WWW、FTP 主机，其完整的计算机名分别为 www.xyz.net、ftp.xyz.net，而这两个主机名对应的是同一个 IP 地址。

默认情况下，主机名的解析过程如图 7-1 所示。

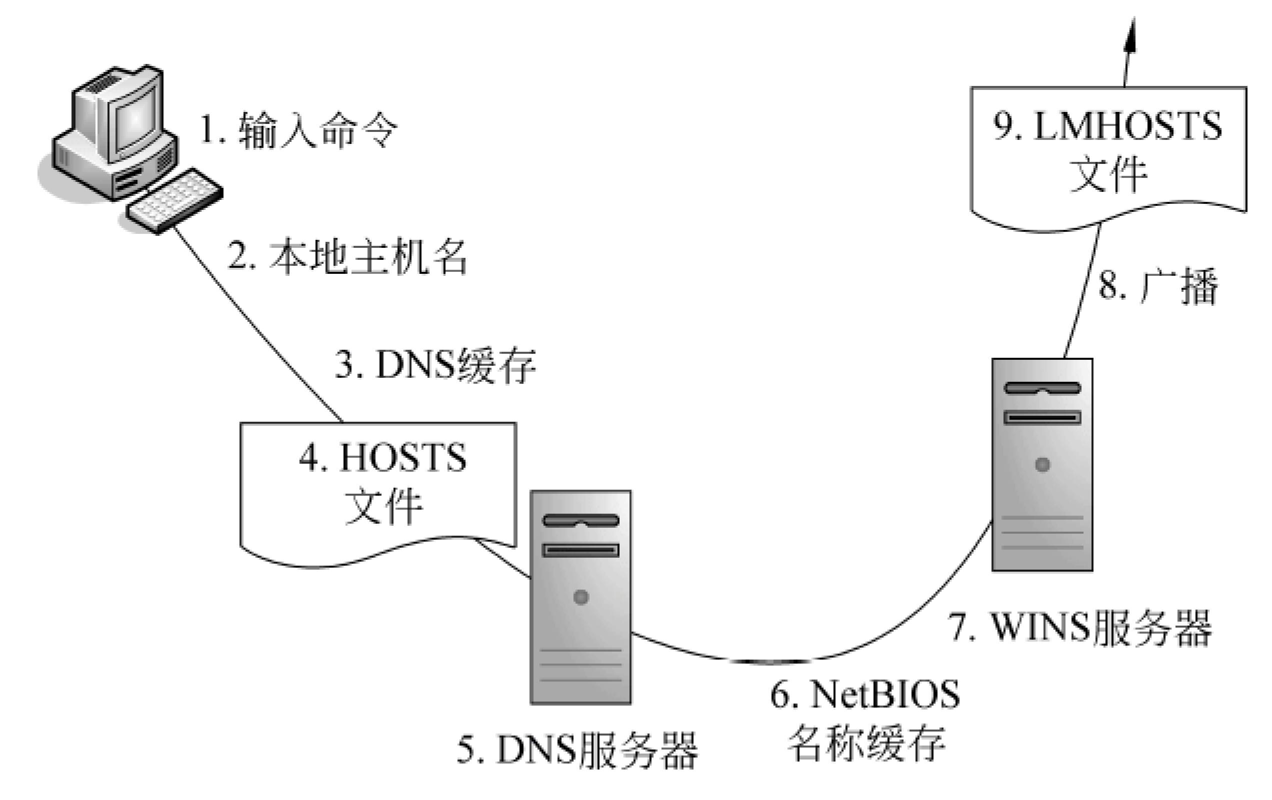


图 7-1　主机名的解析过程

7.2　DNS 命名空间

DNS 全称为 Domain Name System，整个 DNS 的结构是一个分层的树状结构，因此很容易扩展，这个树状结构称为 DNS 命名空间，如图 7-2 所示。

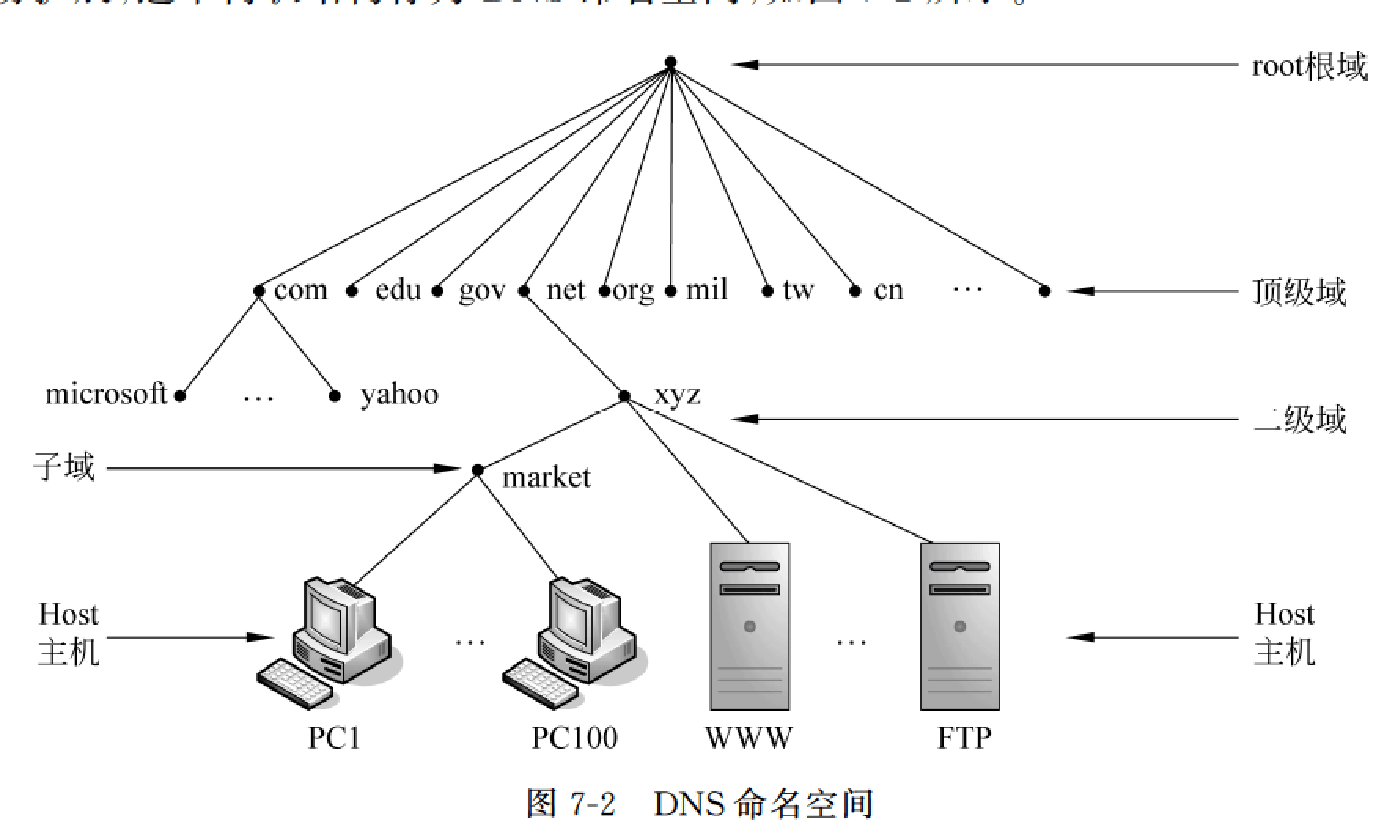


图 7-2　DNS 命名空间

1. 根域

根域位于树状结构的最顶部，用一个小圆点(.)代表。Internet 中目前有 13 台根 DNS 服务器，它们由多个机构负责管理，例如 InterNIC 等。

2. 顶级域

顶级域位于根域之下，由 2～3 个英文字母组成。常见的顶级域名如表 7-1 所示。

表 7-1　常见的顶级域名

顶 级 域 名	说　　明
com	适用工商金融企业
edu	适用于教育、学术研究单位
gov	适用于官方政府单位
net	适用于网络服务机构
org	适用于财团法人等非盈利机构
mil	适用于国防军事单位
biz	适用于商业机构
info	适用于所有用途
占两个字符的地区及国家码	例如 cn 表示中国

3. 二级域

二级域名位于顶级域名之下，供公司、组织或个人申请、注册。例如，域名 microsoft.com 是由 Microsoft 公司注册的。在二级域之下，可以再划分更多的子域。例如，在某公司的 xyz.net 域下，为人力资源部建立了一个子域，域名为 hire.xyz.net，子域域名的后缀必须是其父域的域名，即子域必须和其父域有连续的命名空间。

4. 主机名称

主机名称用于识别 Internet 或局域网中的特定的计算机。例如，有一个完整的计算机名称 www.xyz.net，其中 www 是主机名称（或别名）代表了这台主机在树状结构中的确切位置。

7.3　安装 DNS 服务器

在 Windows Server 2003 上安装 DNS 服务器之前，要求为该服务器分配固定的 IP 地址，即手工输入 IP 地址、子网掩码、默认网关等信息。

将 Windows Server 2003 独立服务器升级为域控制器时，若安装程序找不到 DNS 服务器，则它会提供在此域控制器内安装 DNS 服务器的选项。

要在 Windows Server 2003 上安装 DNS 服务器，操作步骤为：

（1）单击“开始”→“控制面板”→“添加或删除程序”→“添加/删除 Windows 组件”→“网络服务”→“详细信息”。

（2）在图 7-3 中，选取“域名系统(DNS)”组件，单击“确定”按钮。

（3）返回到前一个对话框后，单击“下一步”按钮即可开始安装 DNS 组件。安装过程中可能需要插入 Windows Server 2003 安装 CD。

完成安装后，单击“开始”→“程序”→“管理工具”→DNS 来连接与管理 DNS 服务器。

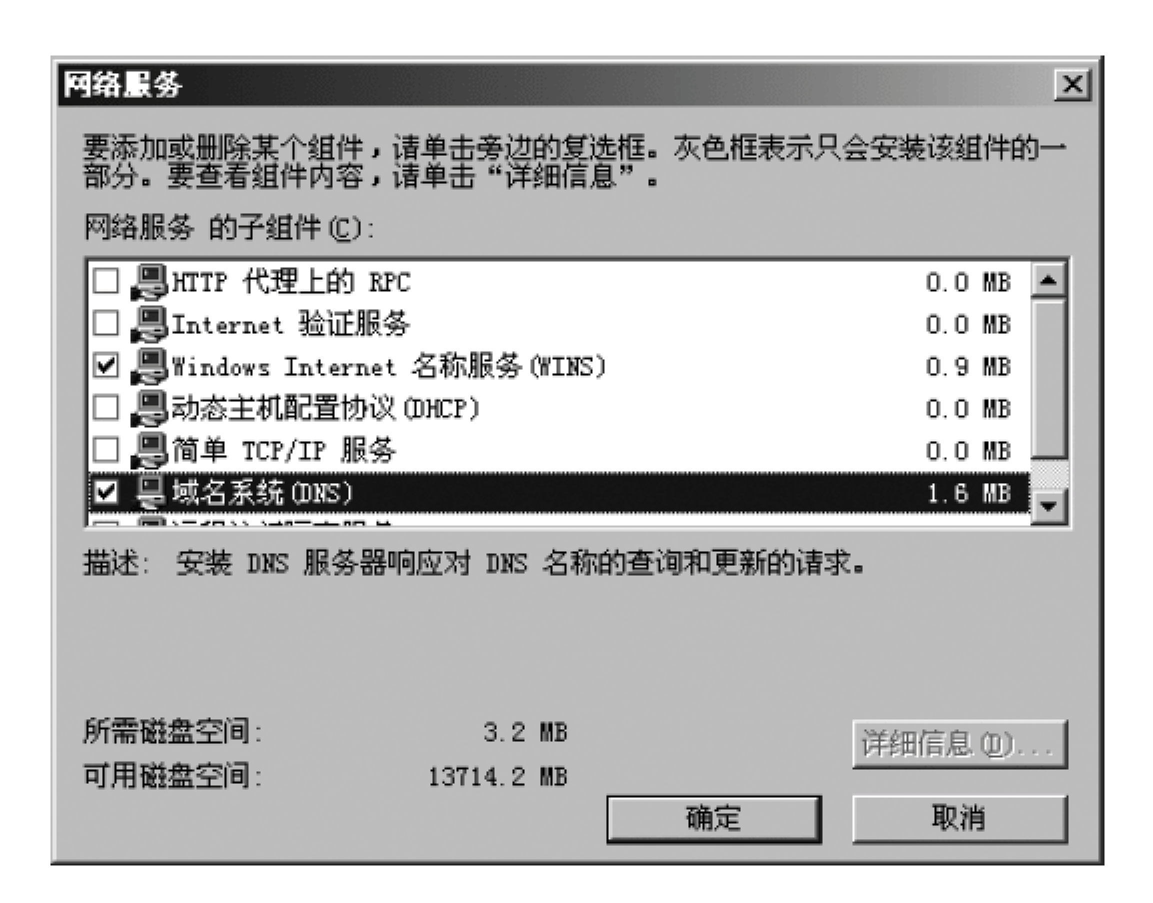


图 7-3 选取域名系统组件

7.4 DNS 查询方式

安装了 DNS 服务器之后，需要建立一个区域，才能完成主机名称解析的服务功能。DNS 区域分为两大类：正向查找区域和反向查找区域。对应于两种查找区域，DNS 查询分为正向查询和反向查询。

1. 正向查询

正向查询用于 FQDN 到 IP 地址的映射，当 DNS 客户端请求解析某个 FQDN 时，DNS 服务器在正向查找区域中进行查找，并返回给 DNS 客户端该 FQDN 对应的 IP 地址。

当 DNS 客户端请求 DNS 服务器查找主机名或域名对应的 IP 地址时，或者此 DNS 服务器向另外一台 DNS 服务器查找主机名或域名对应的 IP 地址时，有两种查找模式。

(1) 递归查询。DNS 客户端向本地的 DNS 服务器发送查询请求后，若此 DNS 服务器没有所需要的记录，则此 DNS 服务器会代替客户端向网络上其他的 DNS 服务器进行查找。一般由 DNS 客户端所提出的查找请求属于递归查询。

(2) 迭代查询。一般 DNS 服务器与 DNS 服务器之间的查找是属于这种查找方式。当第一台 DNS 服务器向第 2 台 DNS 服务器发送查找请求后，若第 2 台 DNS 服务器内没有所需要的记录，则它会提供第 3 台 DNS 服务器的 IP 地址给第一台 DNS 服务器，让第一台 DNS 服务器自行向第 3 台 DNS 服务器进行查找。依次这样找下去，直到找到要查询的主机名对应的 IP 地址。有可能网络上根本不存在这个名称，则查找失败。

当 DNS 客户端向 DNS 服务器 Server01 查找 www.xyz.net 的 IP 地址时，DNS 查询过程如如图 7-4 所示。

(1) DNS 客户端向本地的 DNS 服务器 Server01 查找 www.xyz.net 的 IP 地址(递归查询)。

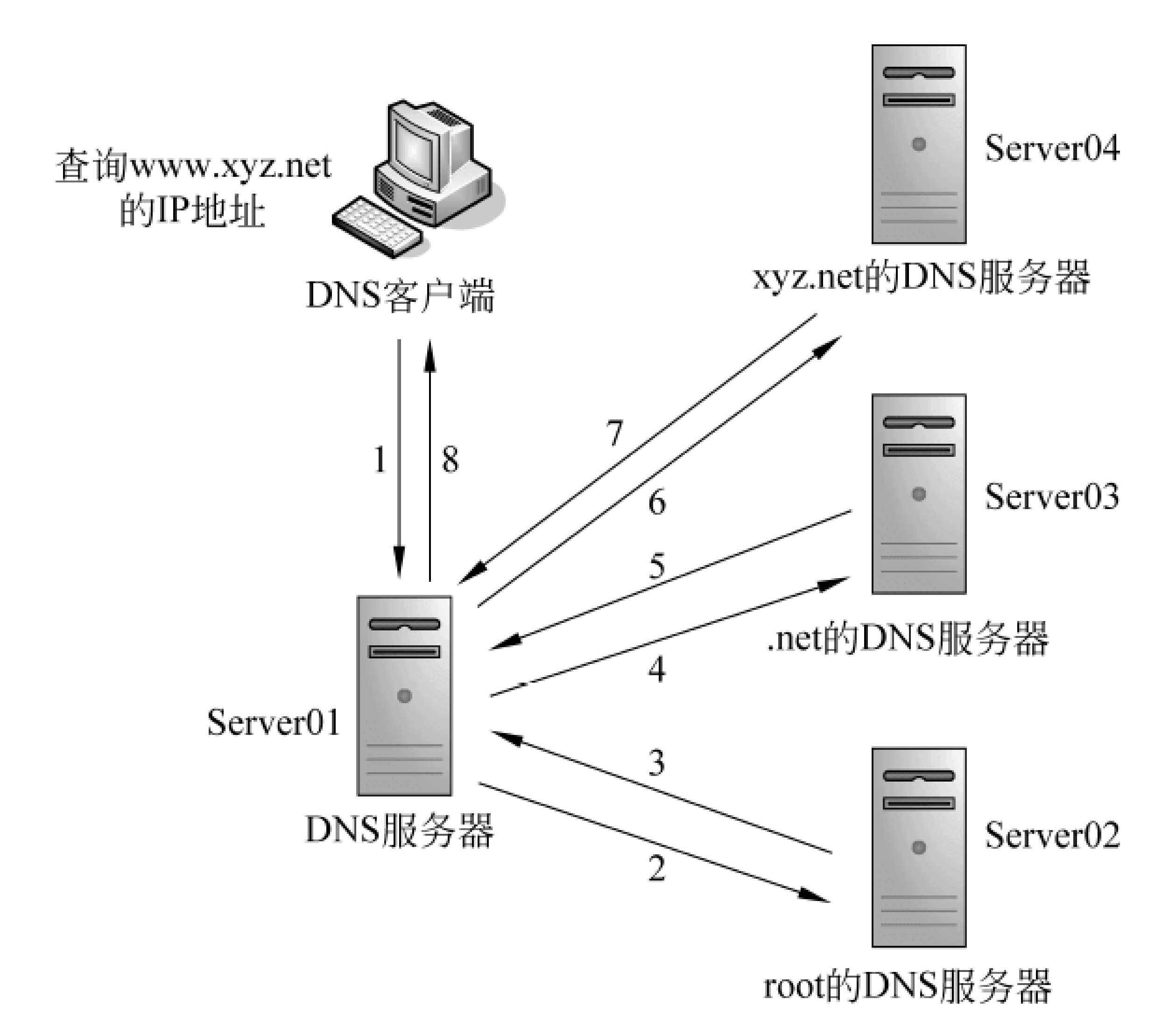


图 7-4 DNS 查询过程

(2) 若 Server01 内没有所要查找的记录,则 Server01 会将此查找请求转发到 root 的 DNS 服务器 Server02(迭代查询)。

(3) Server02 从要查询的主机名称 www.xyz.net 得知,主机位于顶级域.net 之下,因此会将负责.net 区域的 DNS 服务器 Server03 的 IP 地址传送给 Server01。

(4) Server01 得到 Server03 的 IP 地址后,它会直接向 Server03 查找 www.xyz.net 的 IP 地址(迭代查询)。

(5) Server03 从要查找的主机名称 www.xyz.net 得知此主机位于 xyz.net 域之内,因此会将负责 xyz.net 区域的 DNS 服务器 Server04 的 IP 地址传给 Server01。

(6) Server01 得到 Server04 的 IP 地址后,它会向 Server04 查找 www.xyz.net 的 IP 地址(迭代查询)。

(7) 负责 xyz.net 的 DNS 服务器 Server04 将 www.xyz.net 的 IP 地址传送给 Server01。

(8) Server01 再将得到的 www.xyz.net 的 IP 地址传送给 DNS 客户端。

DNS 客户端得到 www.xyz.net 的 IP 地址后,就可以访问 www.xyz.net 了。

2. 反向查询

反向查询与正向查询不同。反向查询用于 IP 地址到 FQDN 的映射。当 DNS 客户端请求解析某个 IP 地址对应的 FQDN 时,DNS 服务器在反向查找区域中,使用 in-addr.arpa 域中添加的专用指针(PTR)记录进行查找,这些 PTR 记录将 IP 地址与 FQDN 匹配。

例如,要得到 IP 地址为 192.168.10.10 的完整的计算机名,将向本地 DNS 服务器发送一个对 10.10.168.192.in-addr.arpa 中的 PTR 记录的一个请求,然后在 DNS 服务器的反向区域中进行解析。

7.5 区域和记录

Windows Server 2003 DNS 服务器允许建立以下 4 种类型的区域。

(1) 主要区域。用来存储此区域内所有记录的正本。在 DNS 服务器内建立主要区域后，可以直接在此区域内新建、修改、删除记录。区域内的记录可以存储在区域文件(在%systemroot%\system32\DNS 文件夹)内，默认的文件名为“区域名称.dns”，例如区域名称为 xyz.net，则区域文件默认的文件名就是 xyz.net.dns，它是符合标准 DNS 规格的一般文本文件。

(2) 辅助区域。辅助区域内的每一项记录都存储在“区域文件”中，不过它存储的是此区域内所有记录的副本，这份副本信息是利用“区域复制”的方式从主 DNS 服务器复制来的。辅助区域内的记录是只读的、不可修改的。如图 7-5 所示，DNS 服务器 B 与 DNS 服务器 C 内都各有一个辅助区域，其内的记录是从 DNS 服务器 A 内复制过来的，即 DNS 服务器 A 是它们的主服务器。

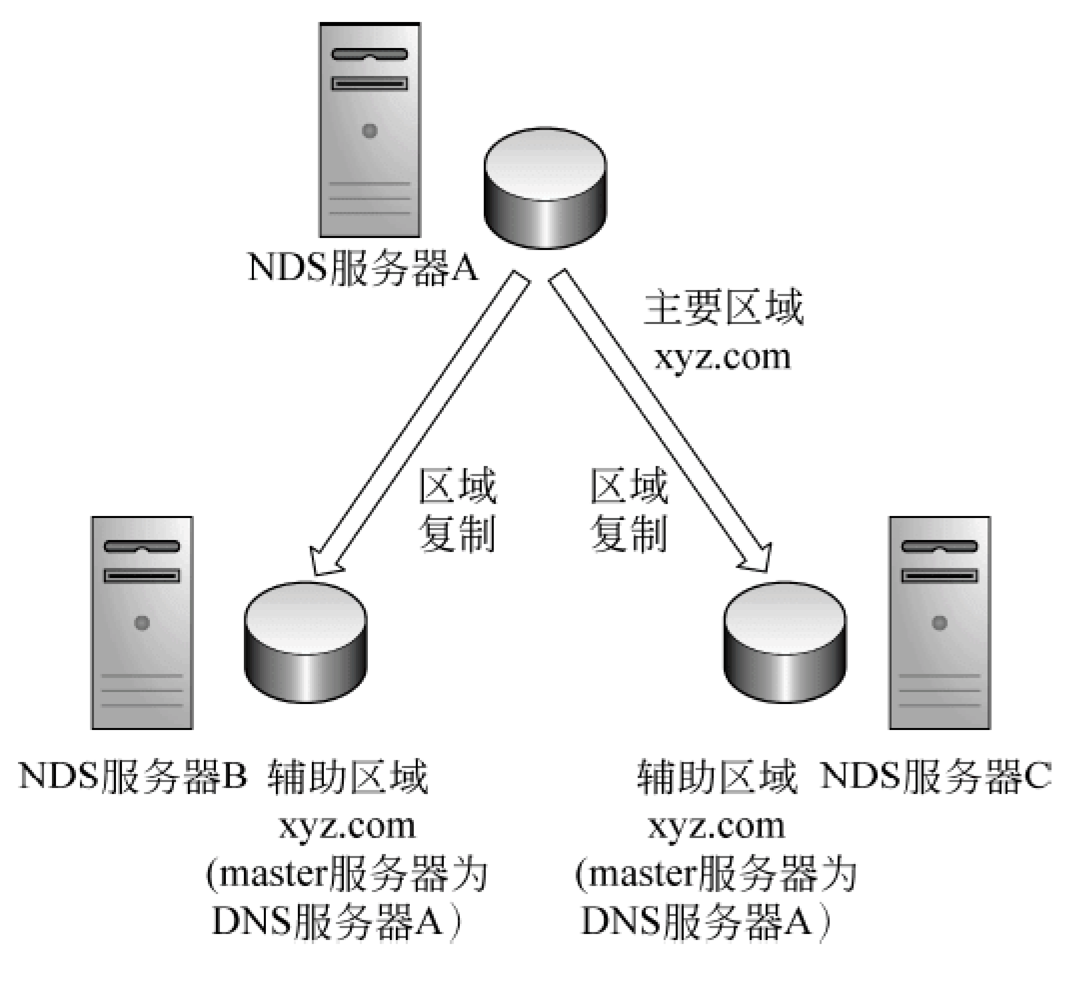


图 7-5 区域复制

(3) 存根区域。存根区域内存储着一个区域的副本信息，不过与辅助区域不同的是，存根区域内只包含少数记录(例如 SOA、NS)，通过这些记录可以找到此区域的授权服务器。

(4) Active Directory 集成区域。在 Windows Server 2003 中，只有在 DNS 服务器是域控制器时才可以使用这种类型。如果 DNS 服务器是域控制器，则可以将记录存储在“区域文件”或 Active Directory 数据库内。若将记录存储到 Active Directory 数据库内，此区域内的记录也将会随着 Active Directory 的复制自动被复制到其他的域控制器。

1. 建立主要区域

在 Windows Server 2003 的 DNS 服务器中，要新建一个主要区域，操作步骤如下。

（1）单击“开始”→“程序”→“管理工具”→DNS，打开 DNS 管理控制台。

（2）选择“DNS 服务器”→右击“正向查找区域”→选择“新建区域”。

（3）出现“欢迎使用新建区域向导”对话框时，单击“下一步”按钮。

（4）在图 7-6 中，选择“主要区域”单选按钮，单击“下一步”按钮。

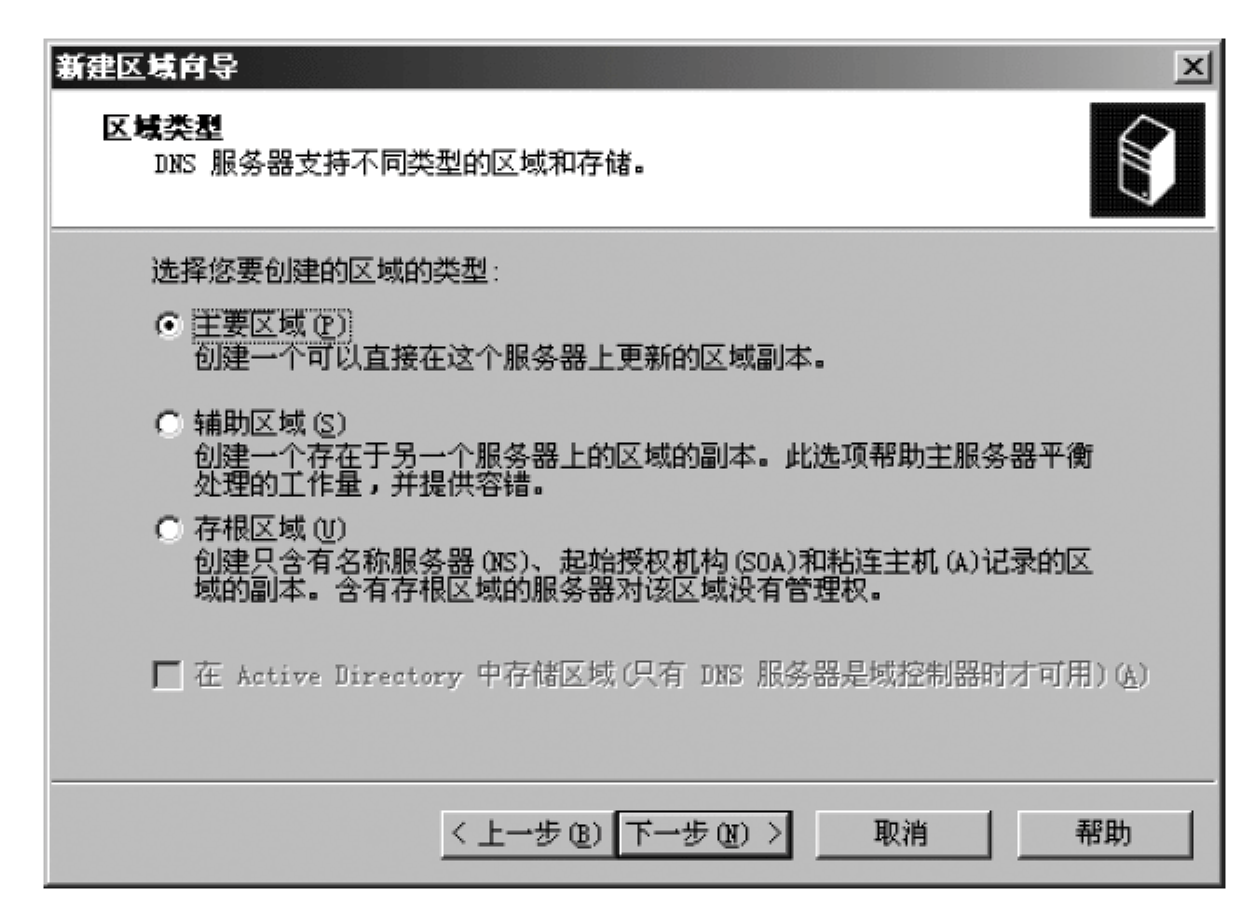


图 7-6　指定区域类型

（5）在图 7-7 中，输入区域名称，例如 xyz.net。区域记录会被存储到区域文件内；如果 DNS 服务器本身是域控制器，而且在上一步中也选择了“在 Active Directory 中存储区域”，则区域记录会被存储到 Active Directory 数据库内。单击“下一步”按钮。

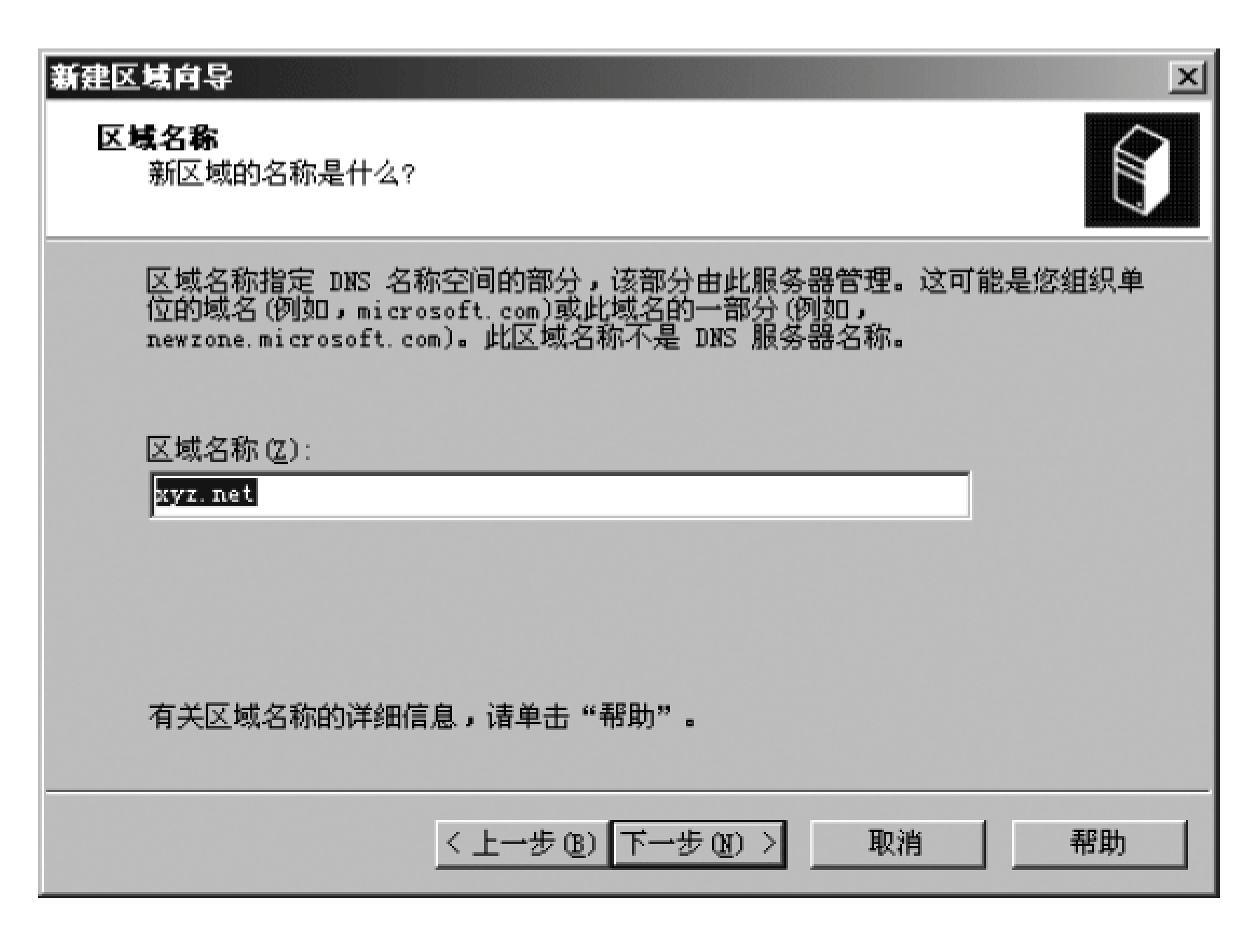


图 7-7　指定区域名称

（6）在图 7-8 中，使用默认的区域文件名称。如果要使用现有的区域文件，则先将该文件复制到%systemroot%\system32\dns 文件内，然后选择“使用此现存文件”单选按钮，并输入文件名称。在此创建新文件，单击“下一步”按钮。

（7）在图 7-9 中，指定 DNS 区域允许接受的动态更新类型，一般选择“不允许动态更新”单选按钮，单击“下一步”按钮。

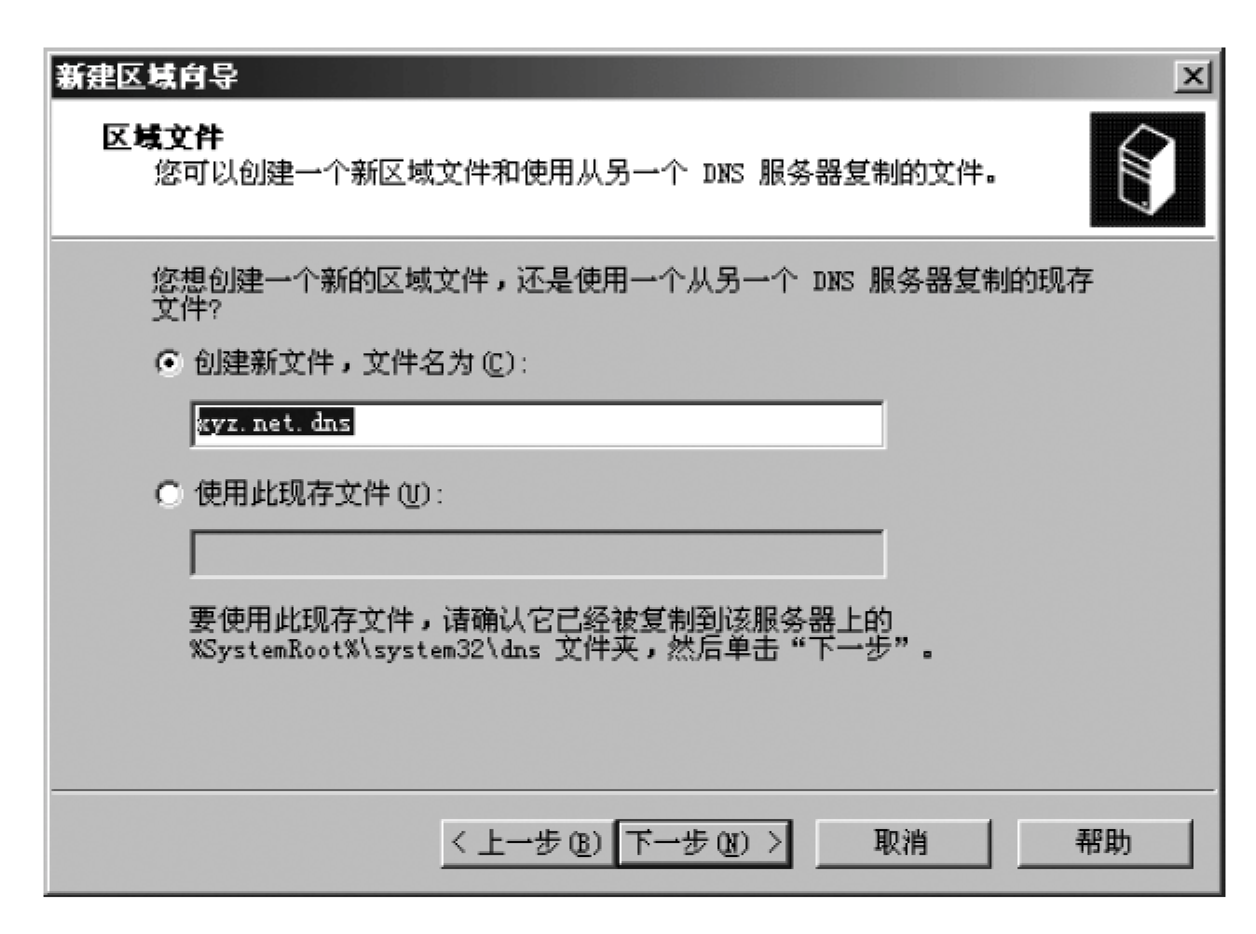


图 7-8　指定区域文件

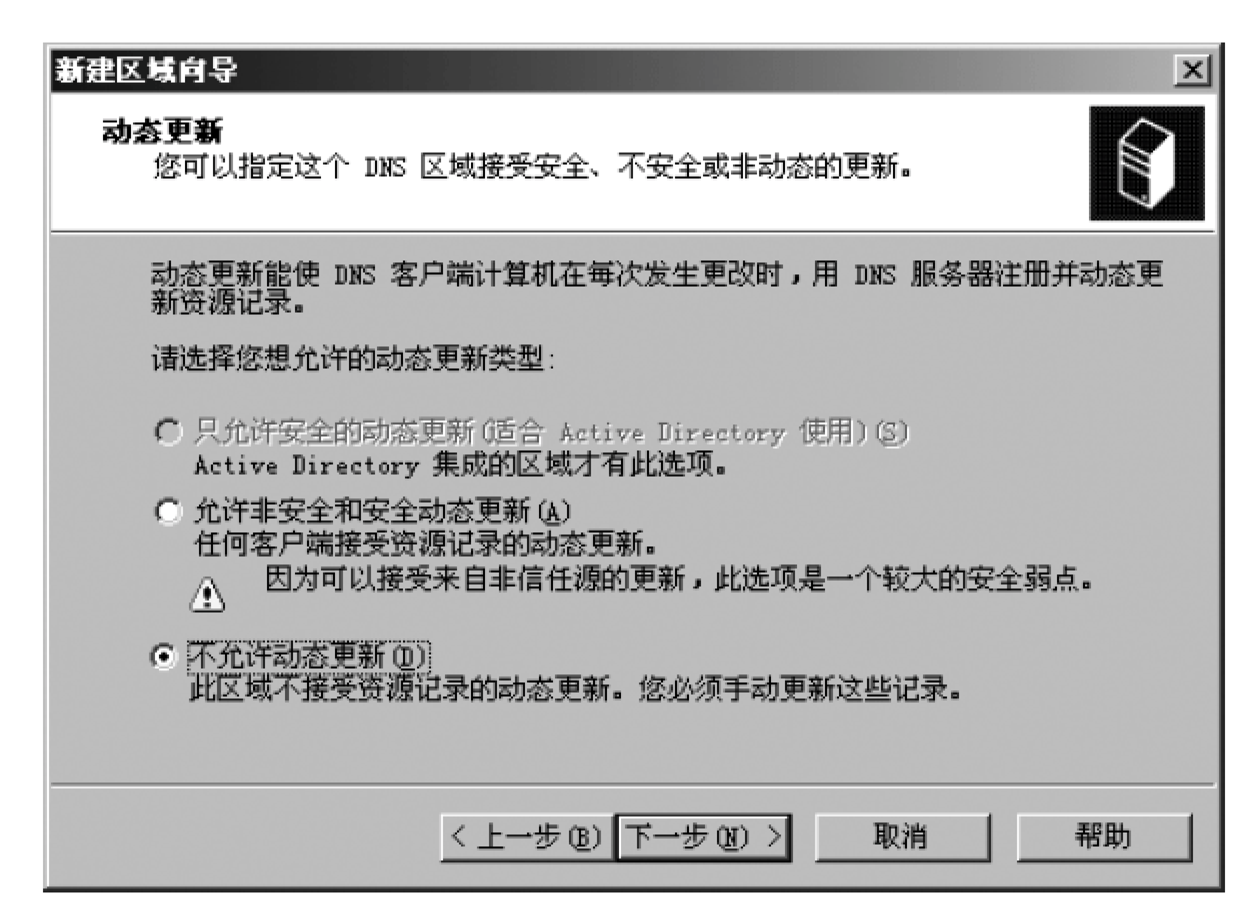


图 7-9　指定动态更新类型

（8）在“完成新建区域向导”对话框中，单击“完成”按钮。成功新建 xyz.net 区域后，如图 7-10 所示。



图 7-10　正向查找区域

2. 在正向查找区域内新建资源记录

成功建立 DNS 区域后，要对外提供名称解析，还要在相应的区域内建立资源记录，即建立主机名称与 IP 地址的映射。DNS 服务器支持多种不同类型的资源记录，在此只介绍常用的资源记录。

1）新建主机记录(A)

要在区域 xyz.net 内新建 www 主机记录，操作步骤如下。

右击区域 xyz.net→选择“新建主机”。在图 7-11 所示的对话框中，在“名称”中输入新建主机记录的名称，只填写 www，而不是 www.xyz.net。在“IP 地址”中输入该主机对应的 IP 地址。如果此 IP 地址与 DNS 服务器在同一子网内，并且 DNS 服务器已创建反向查找区域，则可以选择“创建相关的指针(PTR)记录”，这样会在反向查找区域同时添加该主机的指针(PTR)资源记录。单击“添加主机”按钮。

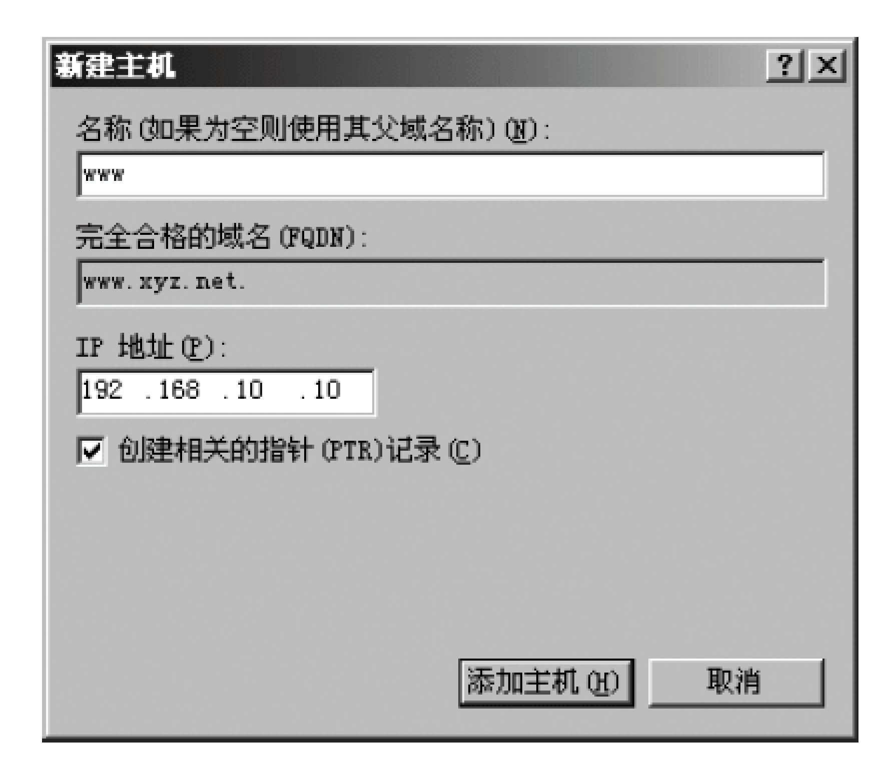


图 7-11 新建主机记录

完成后，如图 7-12 所示。



图 7-12 主机记录

在 DNS 客户端的命令提示符下，执行 ping www.xyz.net 命令，测试是否可以成功解析 www.xyz.net 的 IP 地址 192.168.10.10。重复以上步骤，可以为多台主机在 DNS 服务器的 xyz.net 区域内新建主机记录。

2）新建主机别名记录(CNAME)

要让一台主机拥有多个主机名称，可以为该主机设置别名(Canonical Name，CNAME)，例如，一台主机作为 Web 服务器使用时，其主机名为 www.xyz.net，同时又将其作为 SMTP 服务器，这时其主机名为 smtp.xyz.net。

建立主机别名的操作步骤为：在 DNS 控制台中，右击区域，选择“新建别名”。在图 7-13 中，输入别名 smtp，并单击“浏览”按钮，指定此别名要对应的主机的 FQDN。完成后单击“确定”按钮即可。

在 DNS 客户端利用 ping smtp.xyz.net 命令，测试是否可以成功解析到 smtp.xyz.

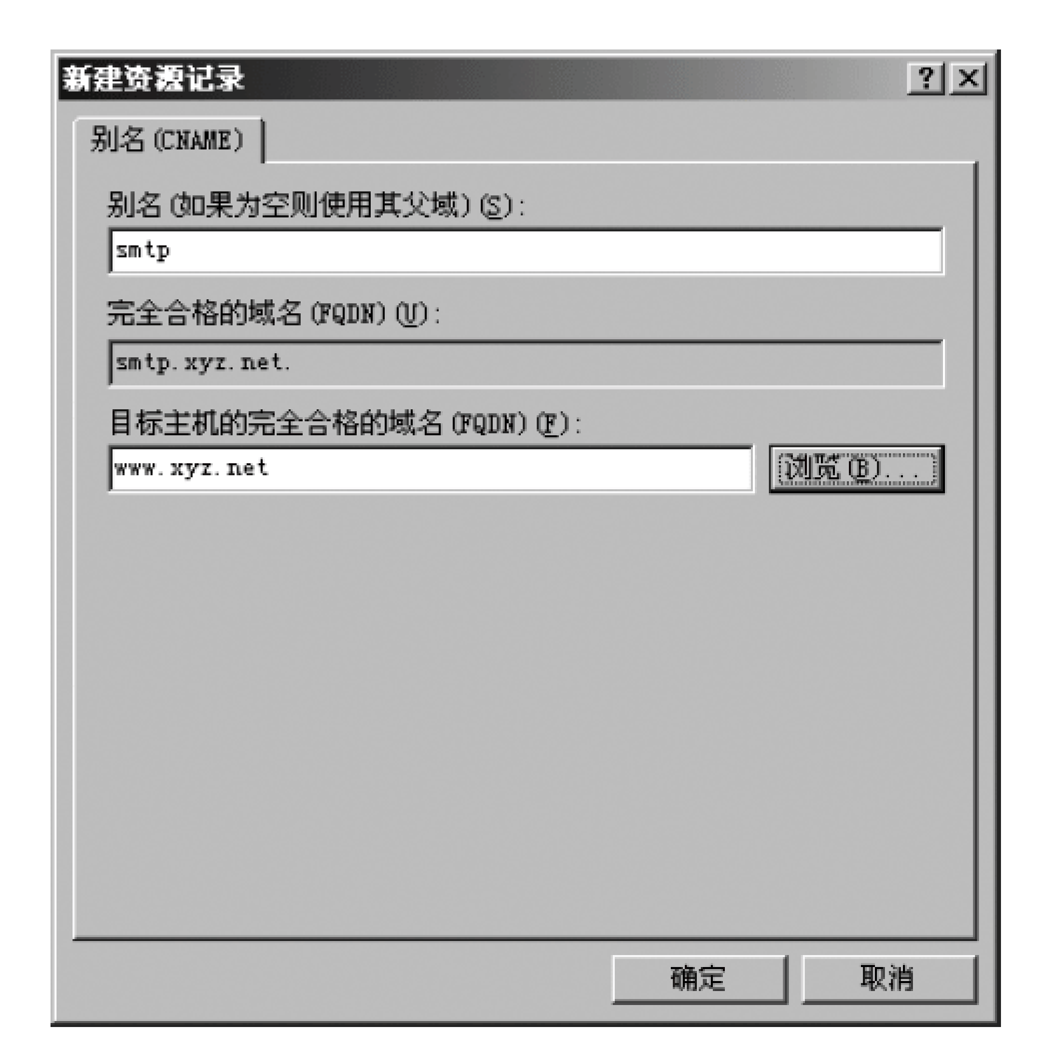


图 7-13　新建别名记录

net 对应的 IP 地址。

3. 建立反向区域与新建反向记录

反向区域可以让 DNS 客户端利用 IP 地址来查找其主机名称。反向查找区域并不是必要的,只是在某些场合下有用。

反向区域的区域名称的前半段是其 Network ID 的反向书写,后半段必须为 in-addr.arpa。若要针对 Network ID 为 192.168.10 的 IP 地址来提供反向查找功能,则此反向区域的名称必须是 10.168.192.in-addr.arpa。

1) 建立反向区域

要新建一个提供反向查询服务的主要区域,假设该反向区域支持的 Network ID 为 192.168.10,操作步骤如下。

在 DNS 控制台中,右击"反向查找区域",选择"新建区域"。在"欢迎使用新建区域向导"对话框中,单击"下一步"按钮,在图 7-14 中,选择"主要区域"单选按钮,单击"下一步"按钮。

在图 7-15 中,在"网络 ID"文本框中输入 192.168.10,这时会自动在"反向查找区域名称"处显示区域名称。也可以在"反向查找区域名称"处输入区域名称。完成后单击"下一步"按钮。

在图 7-16 所示的对话框中,使用默认的区域文件名称。如果要使用现存的区域文件,则必须先将该文件复制到%systemroot%\system32\dns 文件夹内,然后选择"使用此现存文件"。单击"下一步"按钮。

在图 7-17 中,选择"不允许动态更新"单选按钮,单击"下一步"按钮。

在"完成新建区域向导"对话框中,单击"完成"按钮即可完成反向区域的建立。

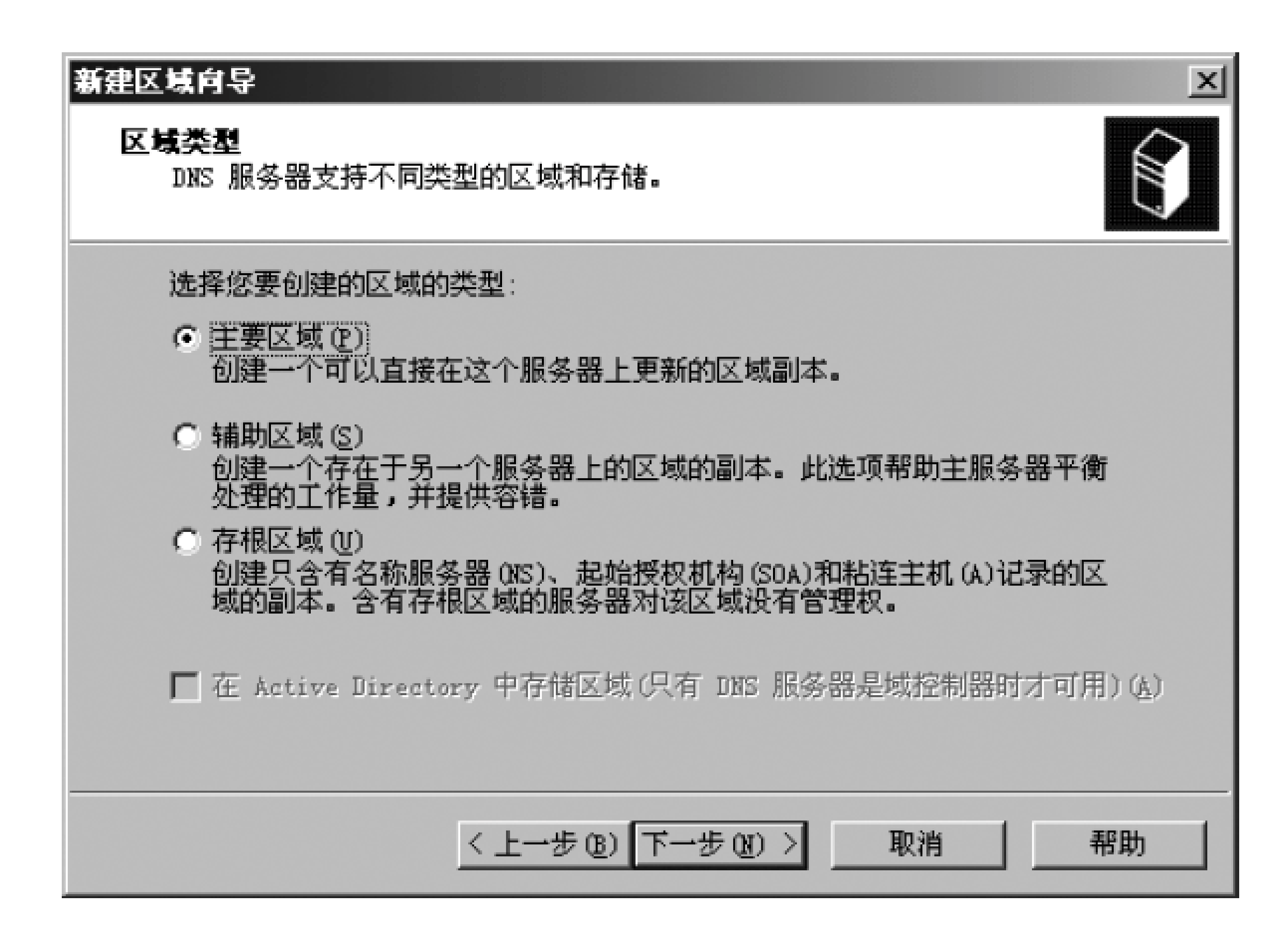


图 7-14　指定区域类型

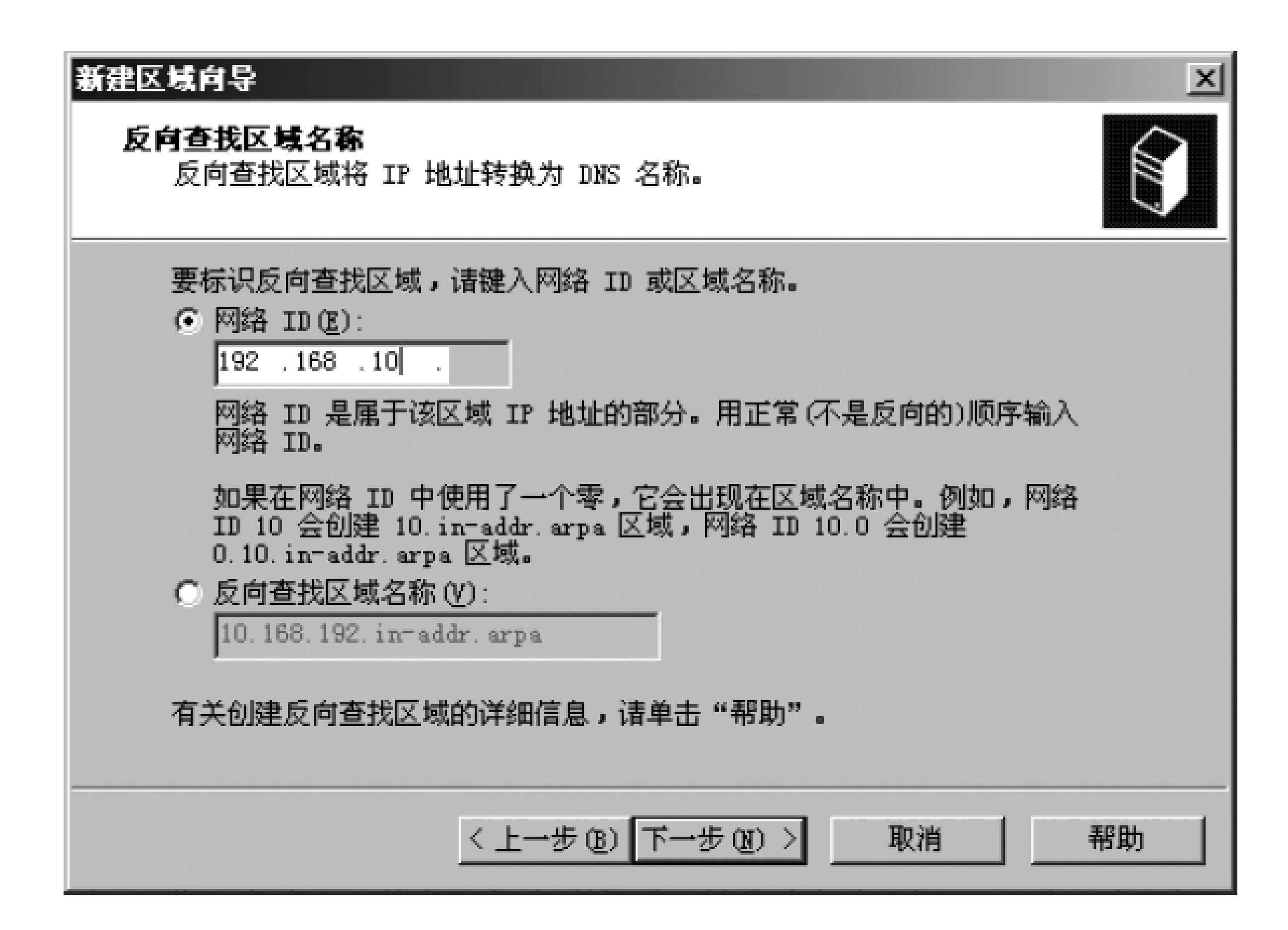


图 7-15　指定反向查找区域名称

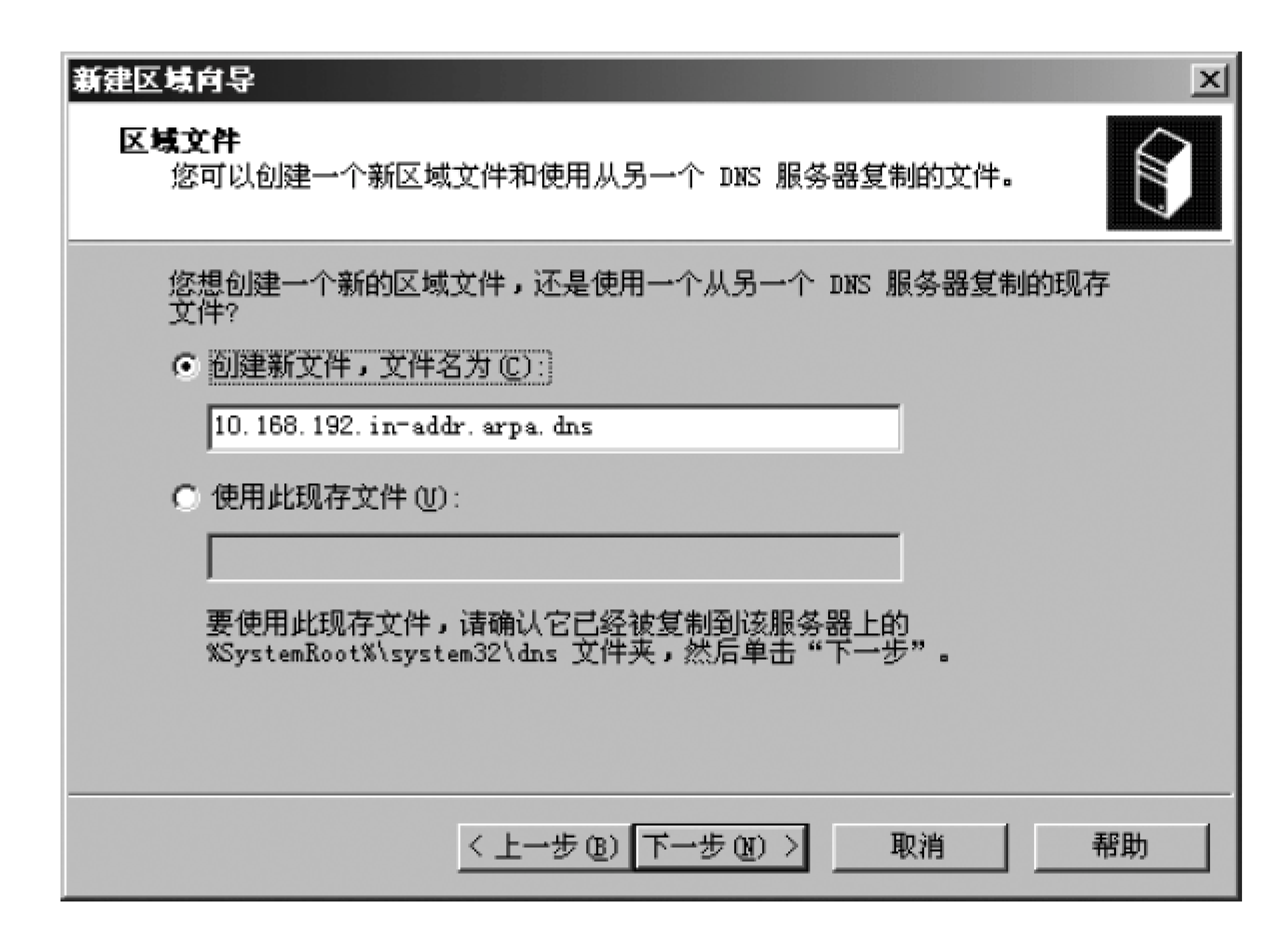


图 7-16　指定反向查找区域文件名

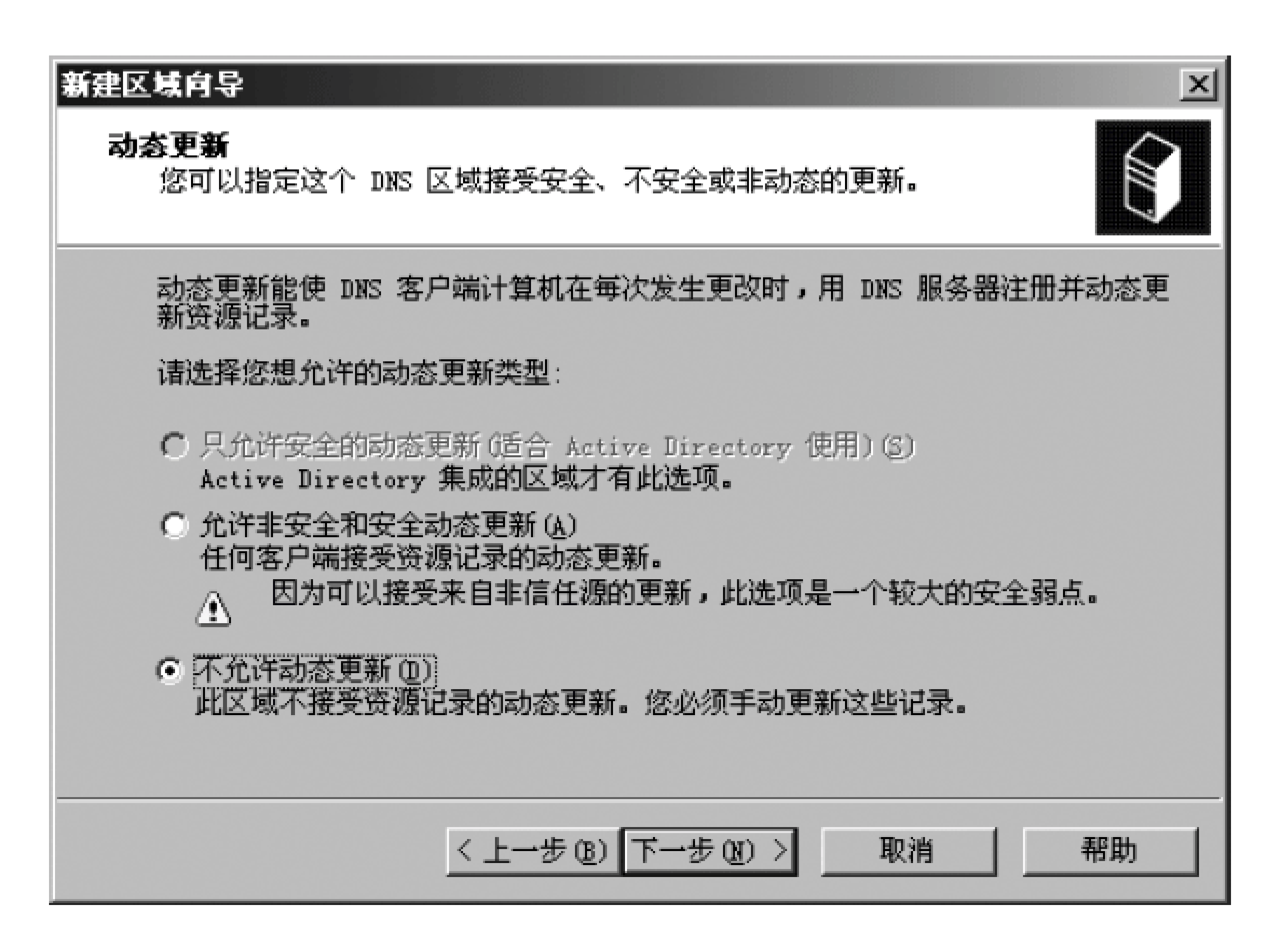


图 7-17　指定动态更新类型

2）在反向区域内建立记录

在反向区域内新建记录的操作步骤如下。

在 DNS 控制台中，右击新建的“反向查找区域”→选择“新建指针(PTR)”。在图 7-18 中，输入“主机 IP 号”，并单击“浏览”按钮指定该 IP 对应的 FQDN。

也可以右击正向区域，选择“新建主机”。在正向区域内建立主机记录的同时，顺便在反向区域内也建立一项记录，只要选择“创建相关的指针(PTR)记录”即可。选择此选项时，相对应的反向查找区域必须已经存在，例如此处建立的正向查询记录，其 IP 地址为 192.168.10.11，则自动在反向查找区域 10.168.192.x Subnet 必须已经存在，才会成功在其中生成一个反向指针记录，如图 7-19 所示。

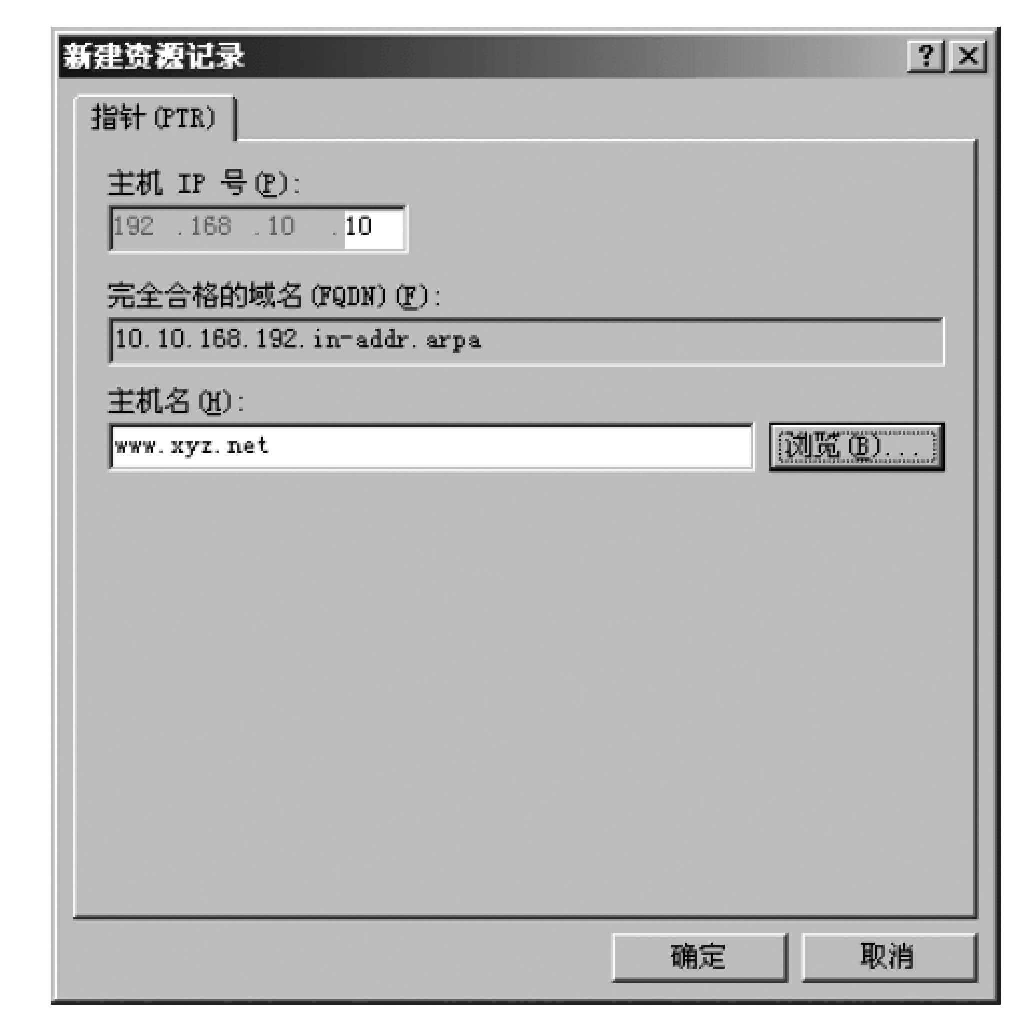


图 7-18　新建指针记录

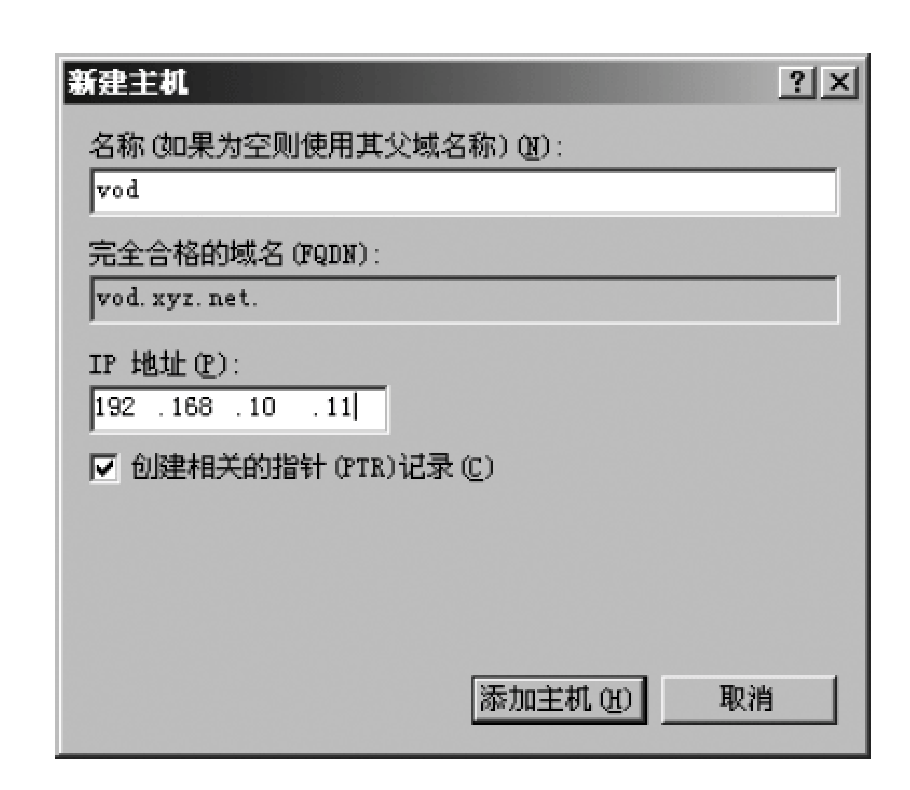


图 7-19　创建相关的指针记录

7.6 配置区域

在 DNS 服务器控制台中，可以更改与区域有关的设置。

1. 常规设置

在 DNS 管理控制台中，右击区域→“属性”选项卡，在“属性”对话框中，更改区域的类型与区域文件名称，以及其他的一些常规管理功能，如图 7-20 所示。

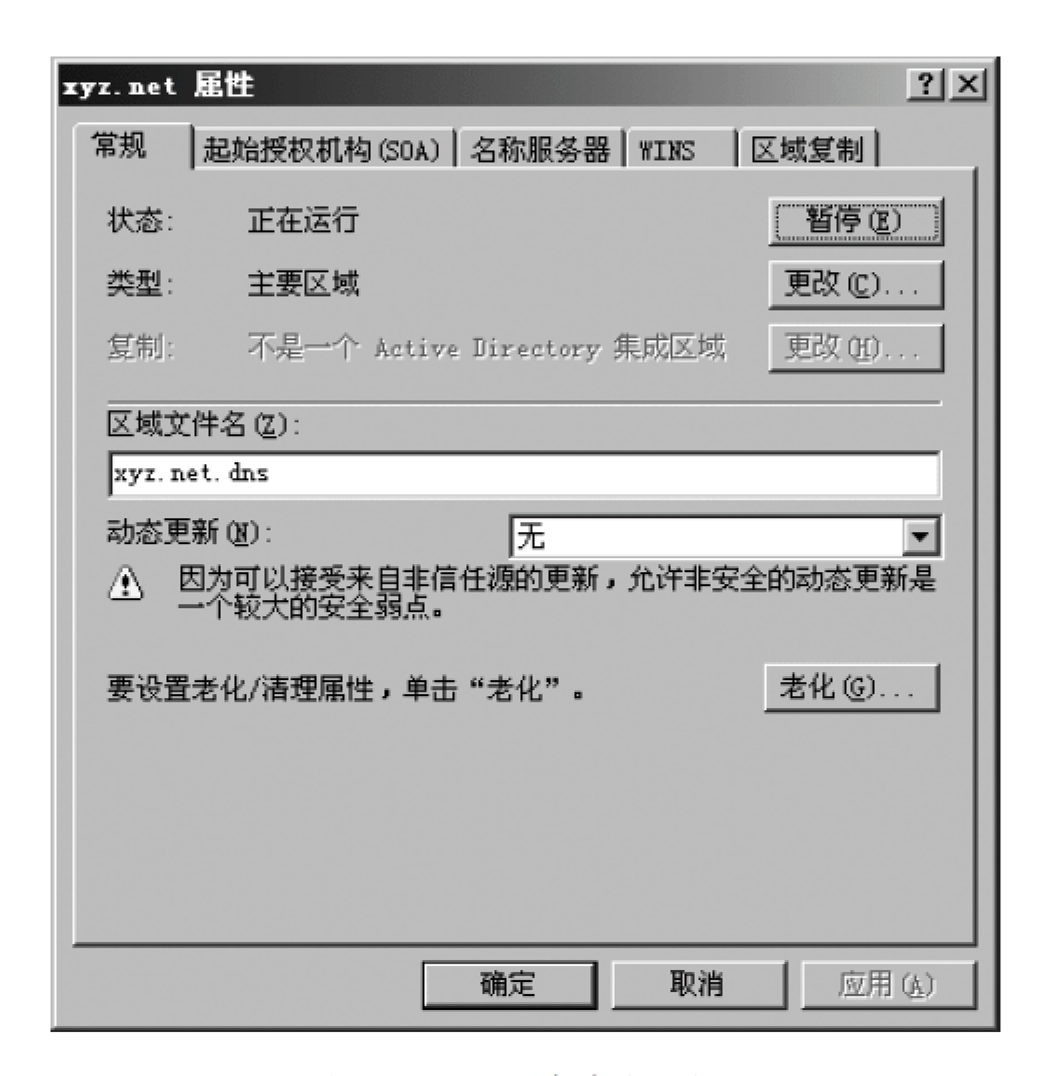


图 7-20　区域常规设置

2. 起始授权机构(SOA)设置

SOA(Start of Authority)用来识别由哪一个 DNS 服务器负责信息授权，在区域数据库文件中，第一笔记录必须是 SOA 的设置数据。SOA 的设置直接影响 DNS 区域的数据更新策略。通过“起始授权机构(SOA)”选项卡，可以修改这些设置，如图 7-21 所示。

3. 名称服务器的设置

在“名称服务器”选项卡中，可以定义名称服务器，如图 7-22 所示。

要添加名称服务器，单击“添加”按钮，在图 7-23 中，单击“浏览”按钮选择名称服务器的 FQDN 或者手工输入，或者在“IP 地址”栏中输入服务器的 IP 地址后，单击“添加”按钮，单击“确定”按钮即可。

图 7-24 显示了名称服务器(NS)记录，“与父文件夹相同”表示与父域名称相同，也就是 xyz.net，因此 xyz.net 的名称服务器是 server01.、www.abc.net. 和 www.xyz.net.。

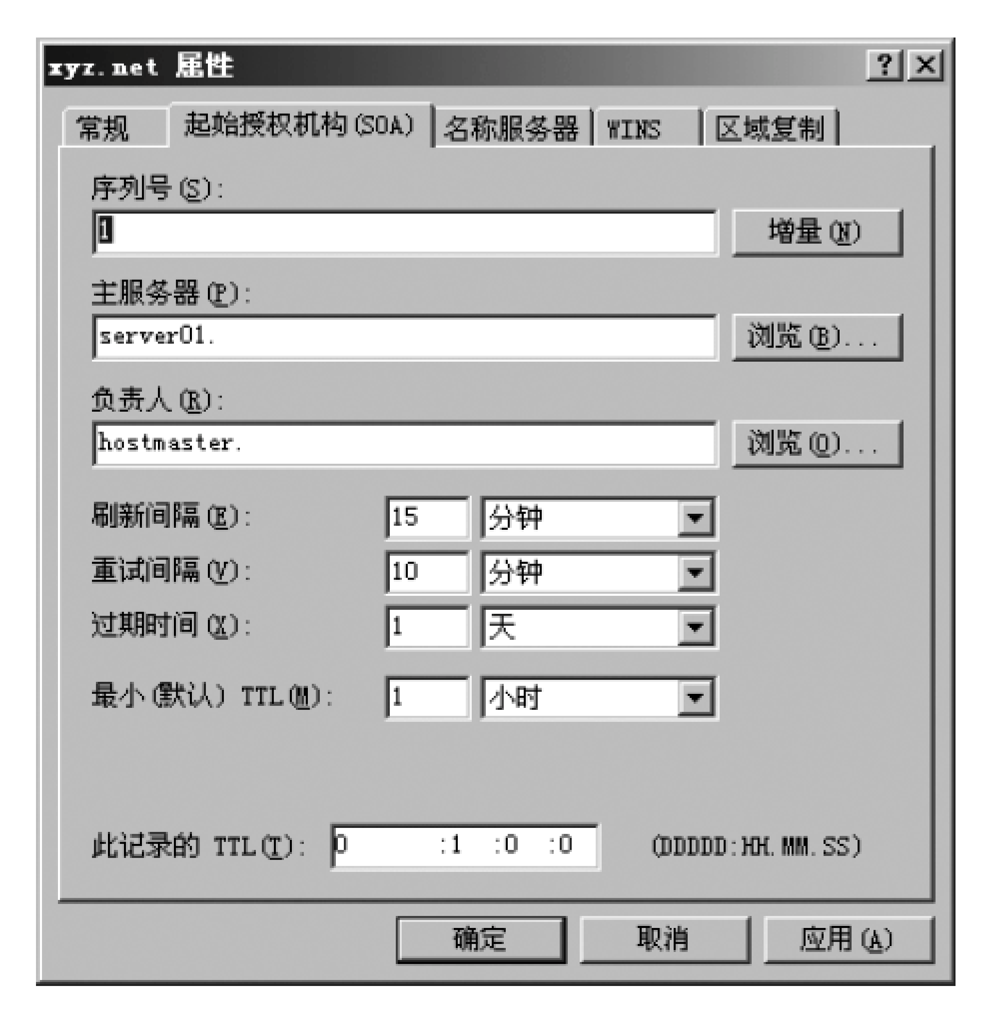


图 7-21　起始授权机构(SOA)设置

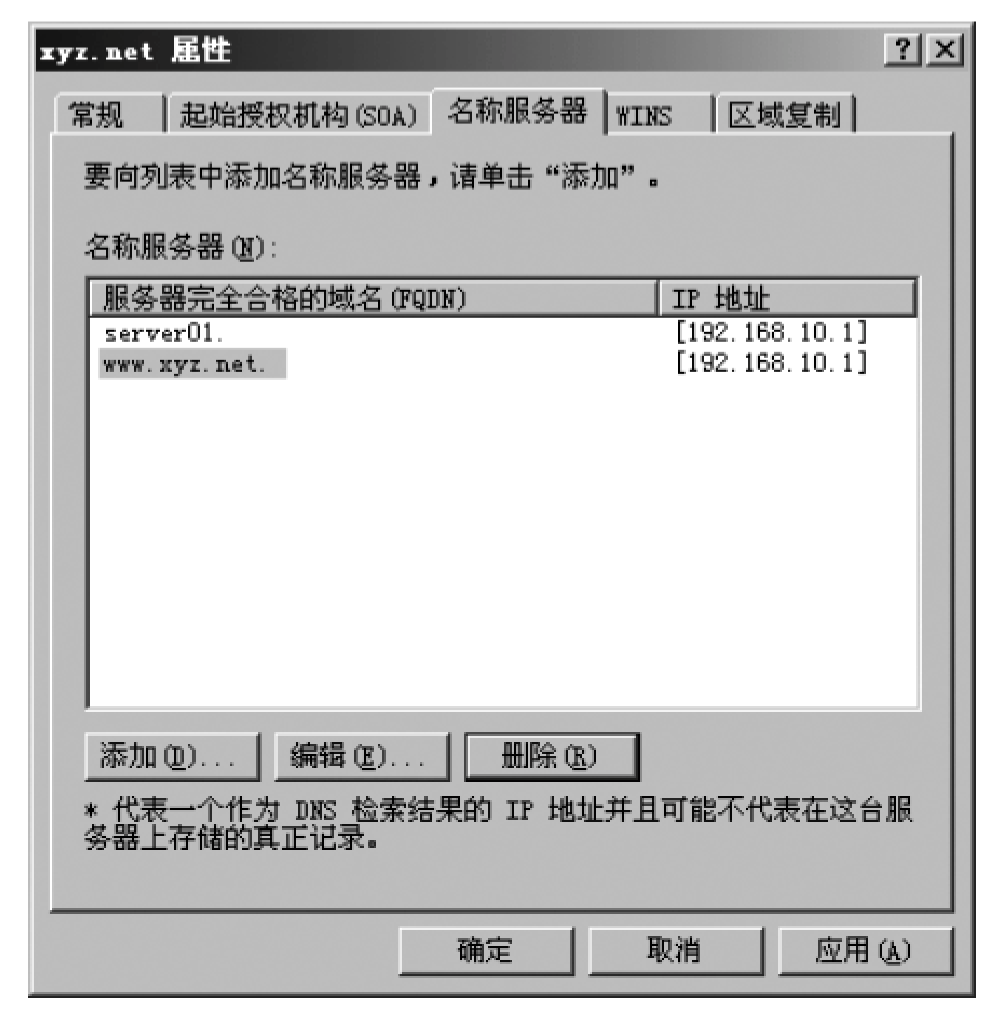


图 7-22　名称服务器的设置

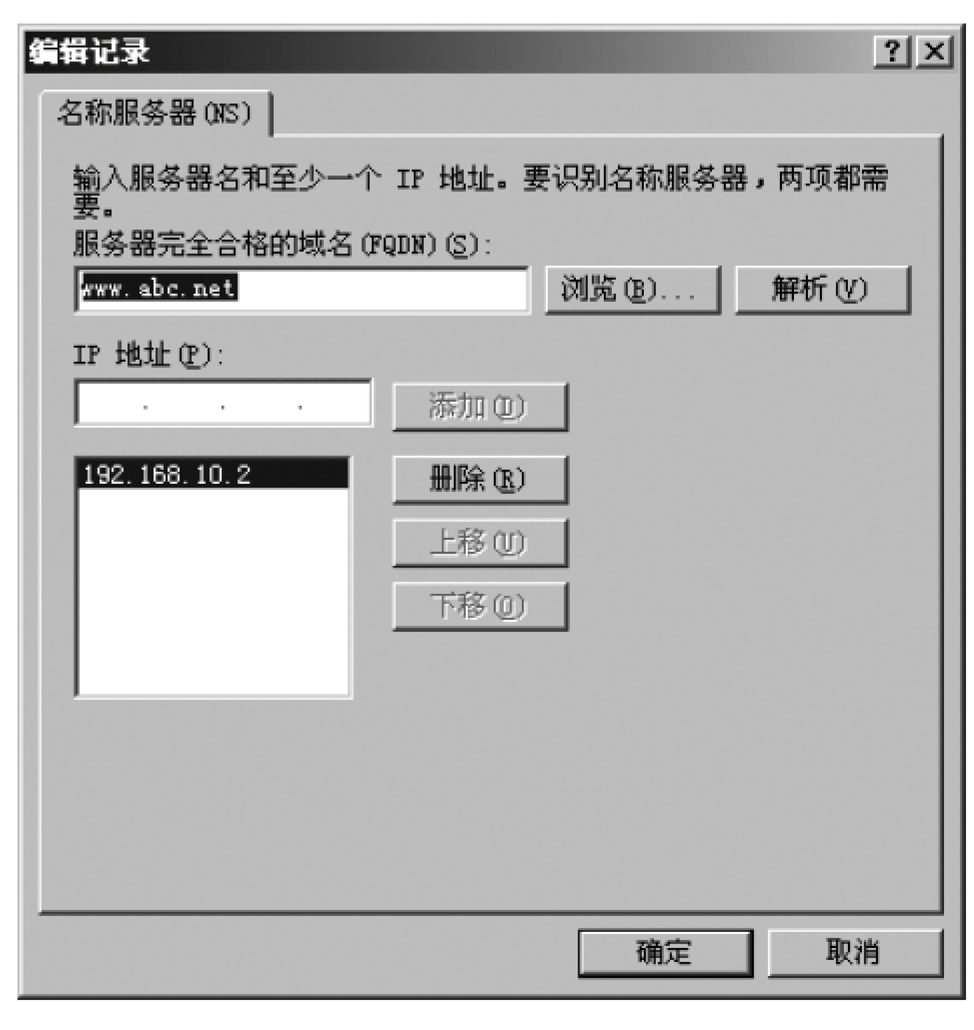


图 7-23　添加名称服务器



图 7-24　名称服务器(NS)记录

4. 区域复制

通过设置主 DNS 服务器与辅助 DNS 服务器之间的区域复制，主服务器可以将区域内的记录只传送到指定的辅助服务器内，其他未被指定的辅助服务器所提出的区域复制请求将被主 DNS 服务器拒绝。在图 7-25 中，若选择“只有在‘名称服务器’选项卡中列出的服务器”单选按钮，表示只接受列在“名称服务器”选项卡处的辅助服务器提出的区域复制请求。

当主服务器区域内的记录有更新时，可以设置是否自动通知辅助服务器，而辅助服务器一旦接到更新通知，就可以发送区域复制的请求。单击“区域复制”选项卡中的“通知”按钮，可以设置要通知哪些辅助服务器，可以通知指定的服务器或是在“名称服务器”选项卡列表中列出的服务器，如图 7-26 所示。

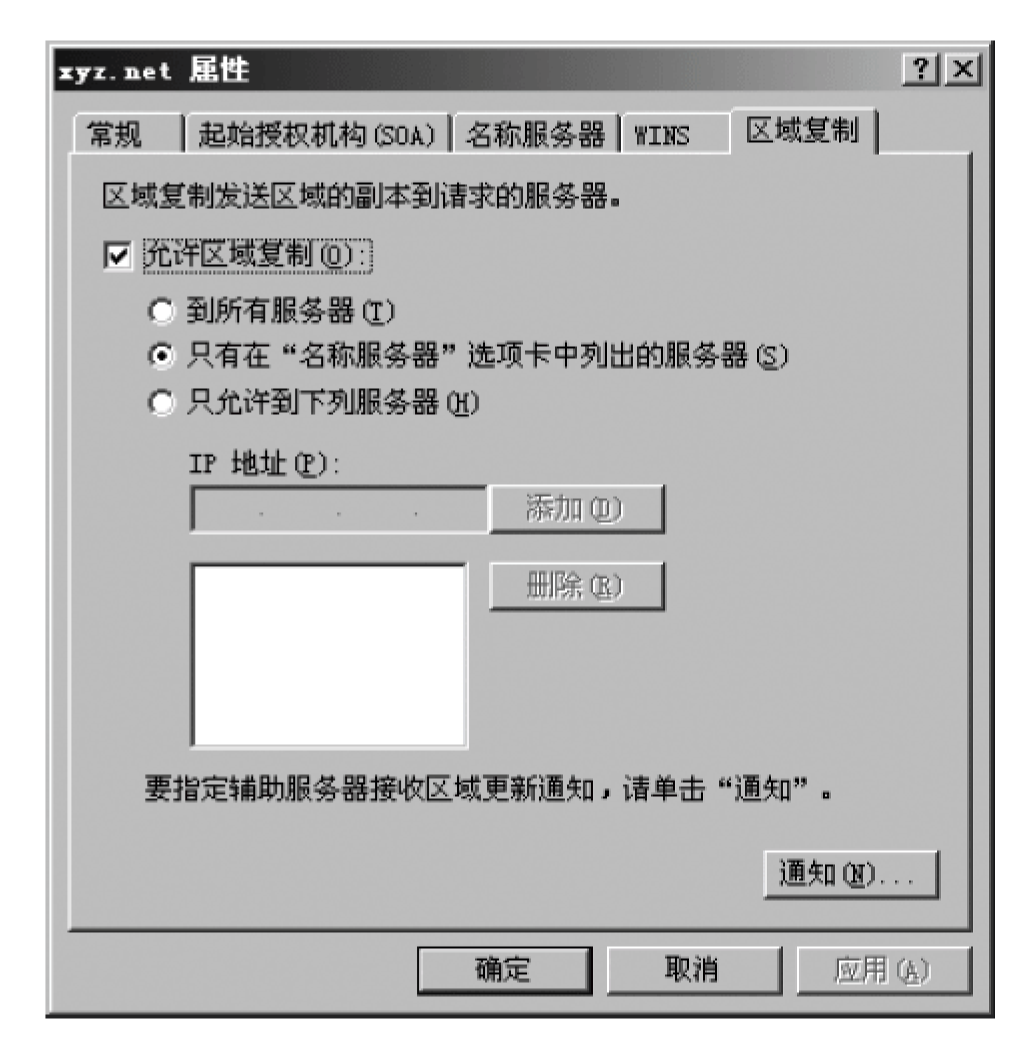


图 7-25　区域复制

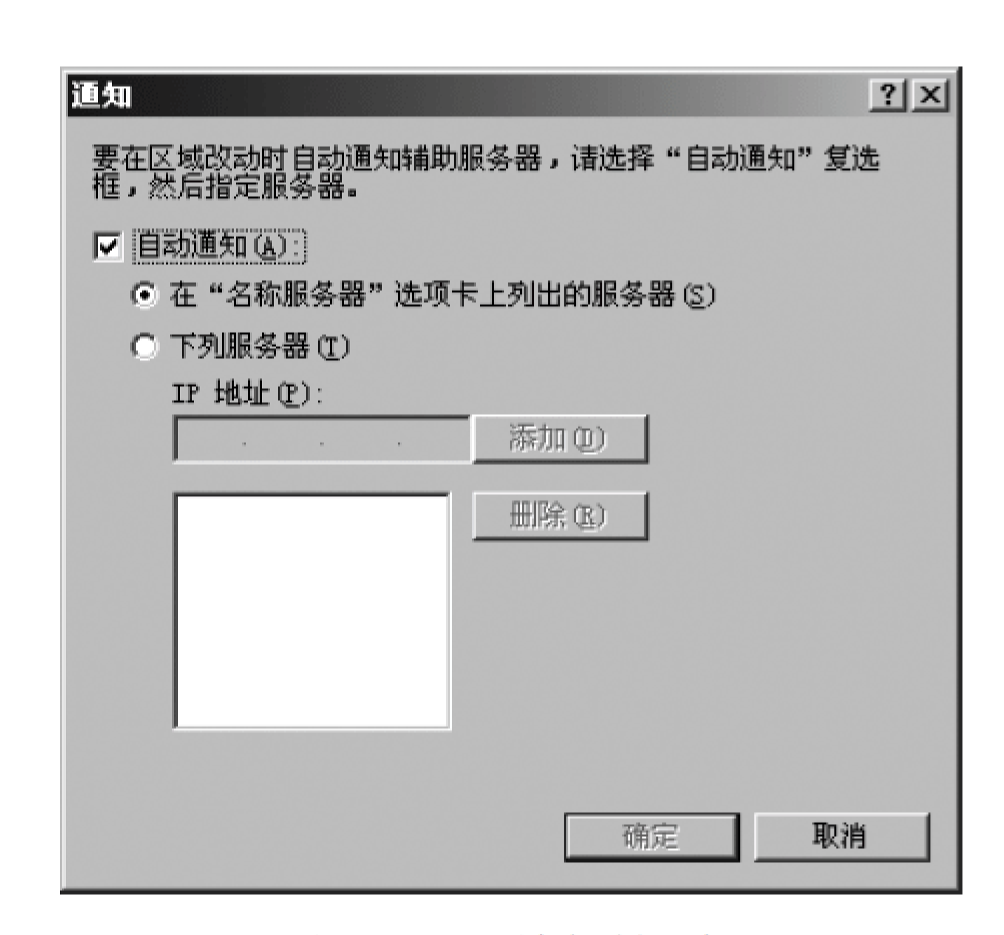


图 7-26　区域复制通知

7.7　DNS 转发

网络上的 DNS 客户端在向本地的 DNS 服务器发送查询请求后，若该 DNS 服务器内没有所需要的记录，则 DNS 服务器会代替客户端向网络上其他的 DNS 服务器发送请求，并负责给客户端返回结果。

可以通过指定 root 服务器和转发器两种方式来查找网络上的其他 DNS 服务器。

1. 指定 root 服务器

DNS 客户端在向 DNS 服务器发送查询请求后，若 DNS 服务器内没有所需要的记录，则 DNS 服务器会代替客户端向 root 内的服务器来查找(除非指定了“转发器”)，可以在 DNS 主控制台中，右击 DNS 服务器→“属性”→“根提示”，如图 7-27 所示，默认情况

下，共有 13 台 root DNS 服务器。



图 7-27　配置根提示

这些信息是从%systemroot%\system32\DNS\cache.dns 文件读取来的。可以在“根提示”选项卡中添加、编辑、删除 DNS 服务器，这些改动信息会被存储到 cache.dns 文件夹内。也可以单击“从服务器复制”，以便从其他的 DNS 服务器复制“根提示”。

如果公司的网络没有连接到 Internet，那么就没有必要利用 root DNS 服务器查找外部主机的名称信息，这时可以在公司 DNS 服务器的“根提示”选项卡下，删除所有默认的 DNS 服务器。同时，可以将“根提示”选项卡下的 DNS 服务器改为公司内部最上层的 DNS 服务器，这样若用户在本部门的 DNS 服务器中查询不到某个主机名时，可以直接转给“根提示”下配置的公司内部的最上层的 DNS 服务器进行查找。

2. 转发器的设置

本地网络中的 DNS 服务器会将它们无法解析的查询转发给网络上其他的 DNS 服务器，或者把客户端对某些域名的解析请求直接转发给特定的 DNS 服务器来解析，网络上其他的 DNS 服务器或特定的 DNS 服务器称为“转发器”。使用转发器可处理区域外的名称解析请求，并提高网络中主机名称的解析效率。

在一个公司内部可能会有多台 DNS 服务器，不过从安全上考虑，在公司的防火墙上通常会设置只允许取一台 DNS 服务器可以直接与 Internet 上的 DNS 服务器通信，而网络内其他的 DNS 服务器都必须通过这台 DNS 服务器和外界通信，从而向 Internet 查询所需要的信息，此时可将这台 DNS 服务器设置为其他 DNS 服务器的“转发器”。

当本地的 DNS 服务器将 DNS 客户端的查询请求转给转发器后，就等待查询结果，并将得到的结果响应给 DNS 客户端。如果转发器无法查询到所需的记录，则 DNS 服务器可能会：①自动向“根提示”内的 DNS 服务器查找；②直接告诉 DNS 客户端找不到要查询的信息。

若要指定转发器，操作步骤为：在 DNS 控制台中，右击 DNS 服务器→选择“属性”→选择“转发器”选项卡，若在此 DNS 服务器的区域内找不到客户端所请求的记录，就会将这个请求转发到 IP 地址为 192.168.10.3 的 DNS 服务器进行解析，如图 7-28 所示。

可以设置条件转发，条件转发就是根据查询的 DNS 域名使用不同的转发器。例如，可以配置 DNS 服务器，将接收到的主机名后缀为 abc.net 的所有查询转发到 IP 地址为 192.168.10.4 的 DNS 服务器，而将其他的所有查询转发到另外一个 DNS 服务器，如图 7-29 所示。

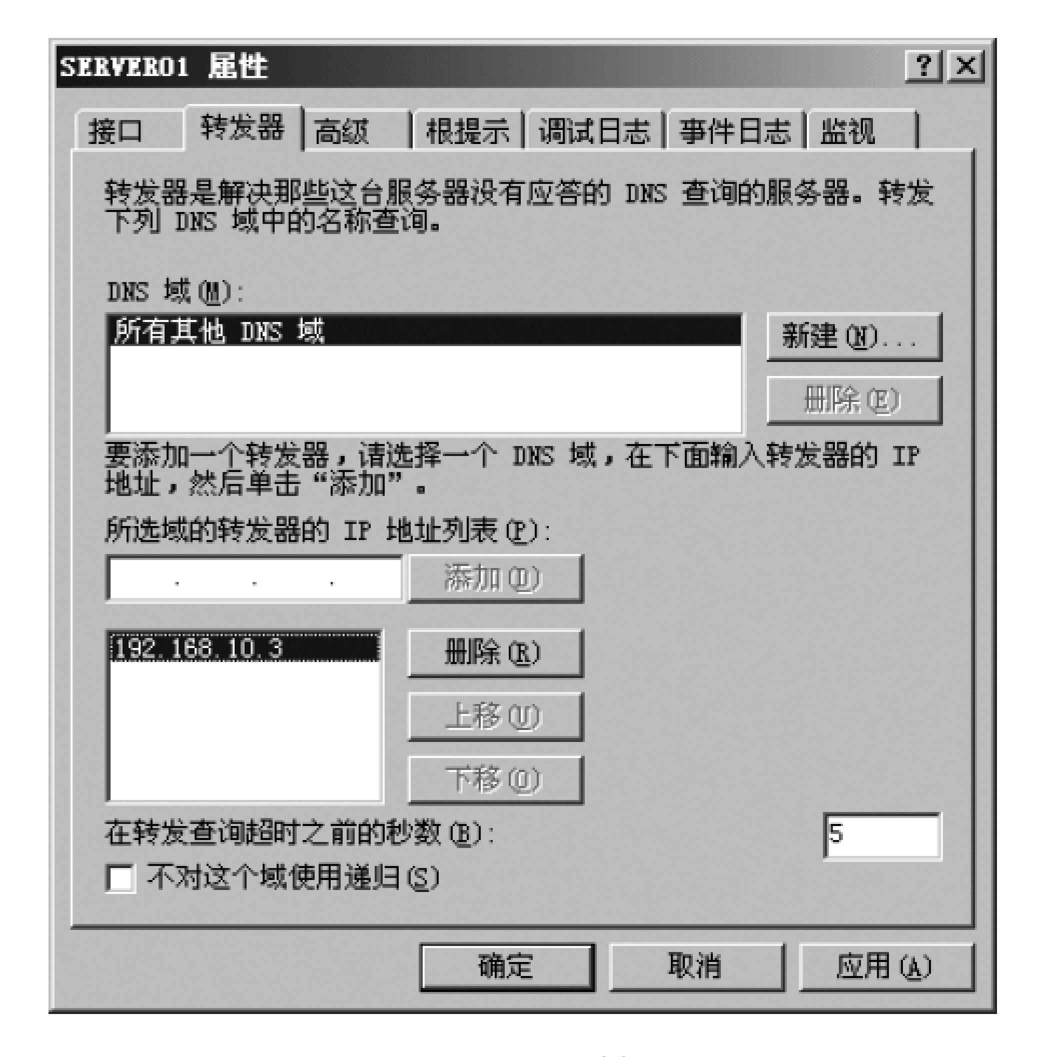


图 7-28　配置转发器

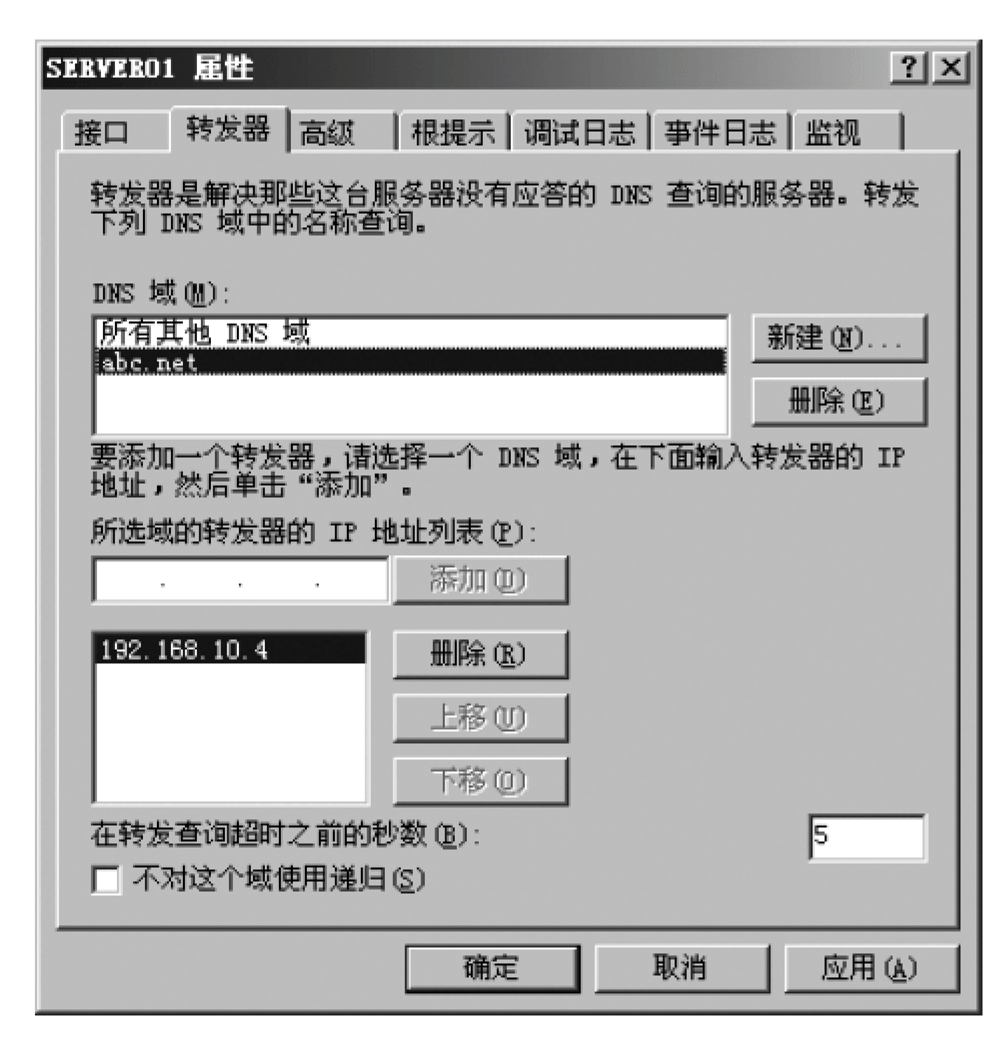


图 7-29　配置条件转发

7.8　DNS 服务器诊断工具

1. 使用 nslookup 命令

nslookup 是 DNS 服务器主要的诊断工具，在安装 TCP/IP 的过程中安装上的，使用 nslookup 命令可以查看发送给任意名称服务器的所有资源记录和直接请求。

nslookup 有两种模式：交互模式和非交互模式。

(1) 如果要求查询多条数据记录，则使用交互模式。在命令提示符下执行 nslookup 命令，不需要参数，输入 exit 则退出交互模式，如图 7-30 所示。

(2) 如果只要求查询一条记录，则使用非交互模式查询。在命令提示符下执行 nslookup {域名/IP} 命令，就能返回结果。例如，由域名查找 IP 地址，在命令提示符下执行 nslookup www.xyz.net。

2. 清除缓存

如果 DNS 服务器的设置与运行一切正常，但是 DNS 客户端无法利用 DNS 服务器来正确解析所需要的 IP 地址，可能是由于 DNS 客户端或是 DNS 服务器缓存内有不正确的

```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>nslookup
DNS request timed out.
    timeout was 2 seconds.
*** Can't find server name for address 192.168.10.1: Timed out
Default Server:  UnKnown
Address:  192.168.10.1

> www.abc.net
Server:  UnKnown
Address:  192.168.10.1

Name:    www.abc.net
Address:  192.168.10.10

>
```

图 7-30　nslookup 命令

信息。

（1）DNS 服务器端缓存的清除。在 DNS 服务器控制台中，右击 DNS 服务器，选择“清除缓存”即可。

（2）DNS 客户端缓存的清除。在 DNS 客户端计算机上，在命令提示符下，执行 ipconfig /flushdns 命令。

第 8 章　DHCP 服务器

学习目标

学习完本章后，了解 DHCP 的工作原理，掌握如何安装和设置 DHCP 服务器，学会如何配置 DHCP 客户端，并掌握 DHCP 服务在路由网络中如何实现。

8.1　配置 IP 地址方式

可以采用以下两种方式为网络中的主机分配 IP 地址与相关配置。

（1）采用静态分配方案，即按照网络管理员的地址规划进行手工设置。

（2）采用基于 DHCP 的动态分配方案，自动为客户端分配 IP 地址、子网掩码、默认网关、DNS 服务器地址以及 WINS 服务器地址等信息，客户端不需要任何设置。

而使用 DHCP 的动态分配方案，也提供两种分配 IP 的方式。

① DHCP 客户端首次从 DHCP 服务器成功租用到 IP 地址之后，就永远使用这个地址。

② DHCP 客户端首次从 DHCP 服务器成功租用到 IP 地址之后，并非永久地使用该 IP 地址，若租约到期，客户端就会释放这个 IP 地址，以供其他客户端使用。也可以更新租约，继续使用原来的 IP 地址。

8.2　DHCP 工作原理

动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）可以减轻 TCP/IP 网络的规划、管理和维护的负担，缓解 IP 地址紧张等问题。

DHCP 服务使用客户/服务器模型。当 DHCP 客户端计算机启动时，它会与 DHCP 服务器通信，以便从 DHCP 服务器获取 IP 地址、子网掩码等配置信息。它们之间的通信方式分为两种情况，即 DHCP 客户端是从 DHCP 服务器获取一个新的 IP 地址还是更新 IP 地址的租约。

DHCP 服务器在网络中的应用如图 8-1 所示。

1. 使用 DHCP 服务器租用 IP 地址

在使用 DHCP 租用 IP 地址的过程中，DHCP 服务器与 DHCP 客户端之间需要发送 4 个数据包来进行通信，如图 8-2 所示。

（1）DHCPDISCOVER。当 DHCP 客户端第一次登录网络时，向网络发送 DHCPDISCOVER 广播包。网络中每一台安装了 TCP/IP 的主机都会接收到这种广播信息，但只有 DHCP 服务器才会做出响应。

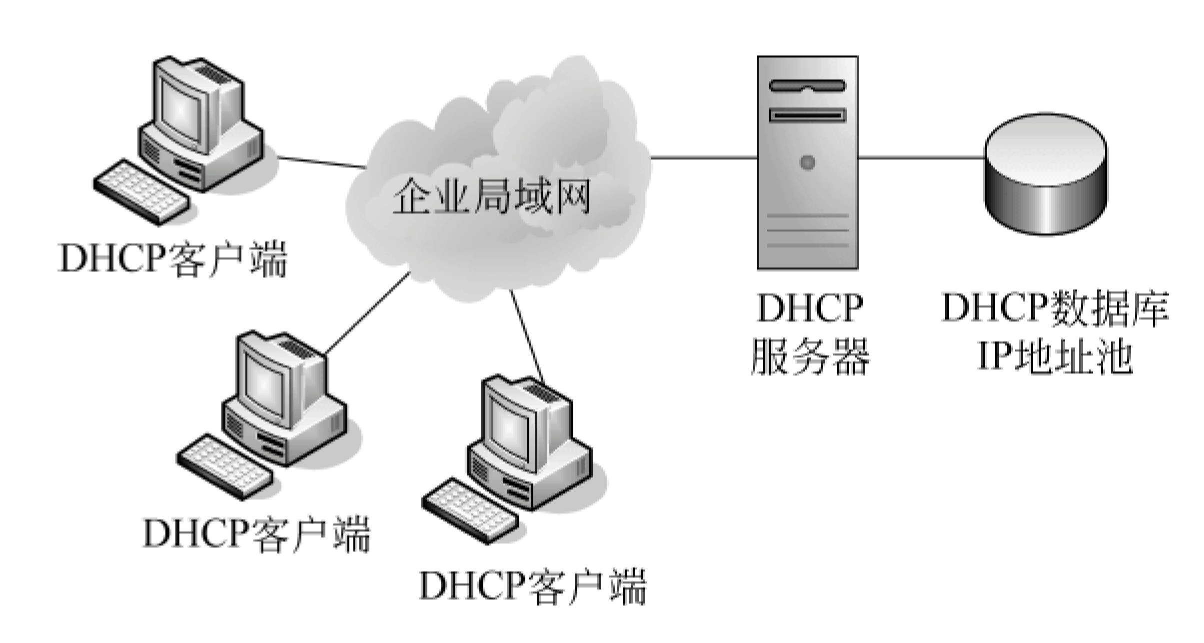


图 8-1　DHCP 服务器在网络中的应用

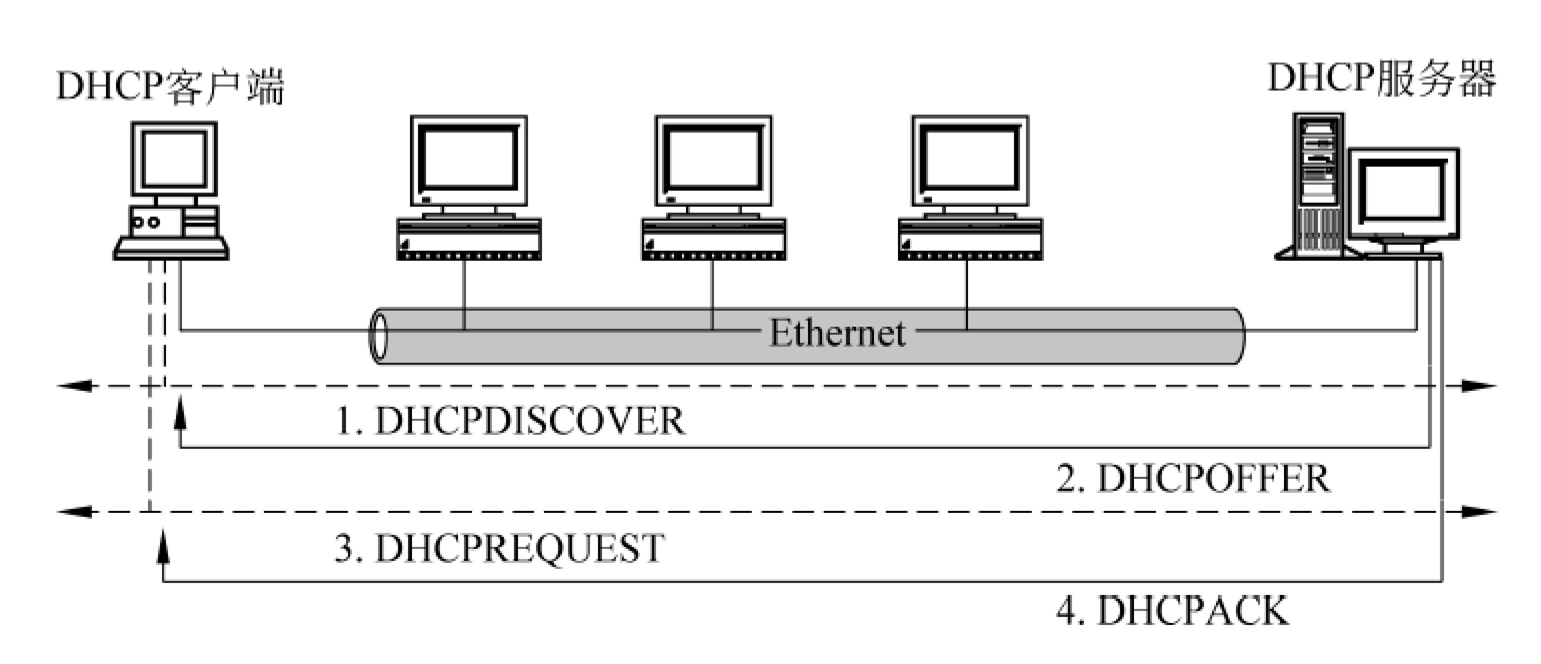


图 8-2　DHCP 服务器与客户端之间的数据包

（2）DHCPOFFER。当 DHCP 服务器监听到客户端发出的 DHCPDISCOVER 广播包后，会从还没有租出的 IP 地址范围内，选择最前面的空置 IP，连同其他 TCP/IP 设置，回应给客户端 DHCPOFFER 广播包。根据服务器端的设定，DHCPOFFER 包还会包含租约期限信息。

（3）DHCPREQUEST。如果 DHCP 客户端接收到了多台 DHCP 服务器的回应，只会挑选其中一台 DHCP 服务器提供的 DHCPOFFER（通常是最先抵达的那个），并且会向网络发送一个 DHCPREQUEST 广播包，通知所有其他 DHCP 服务器它将接受这台 DHCP 服务器提供的 IP 地址，以便其他 DHCP 服务器收回曾经提供给客户端的 IP 地址。同时，客户端还会向网络发送一个 ARP 包，查询网络上有没有其他计算机使用该 IP 地址，如果发现该 IP 地址已被占用，客户端则会送出一个 DHCPDECLINE 封装包给 DHCP 服务器，拒绝接受其 DHCPOFFER，并重新发送 DHCPDISCOVER 包，以便获取一个新的 IP 地址。

（4）DHCPACK。当 DHCP 服务器接收到 DHCP 客户端的 DHCPREQUEST 包后，它便使用广播向 DHCP 客户端发送 DHCPACK 包，包含它所提供的 IP 地址和其他设置，通告 DHCP 客户端可以使用它所提供的 IP 地址。当 DHCP 客户端收到确认信息后，TCP/IP 的初始化过程就完成了，然后 DHCP 客户端就可将其 TCP/IP 的设置与网卡绑定，一旦绑定，就可开始利用 TCP/IP 进行网络通信。

2. IP 地址的更新与释放

当 IP 租约期过一半时，所有的 DHCP 客户端自动试图更新它们的 IP 地址租约期。要更新 IP 地址租约期，DHCP 客户端直接发送 DHCPREQUEST 消息给 DHCP 服务器。如果此地址还是有效地址，则 DHCP 服务器给 DHCP 客户端回应一个 DHCPACK 消息，其中包含新的租约期和其他最新配置参数，如图 8-3 所示。

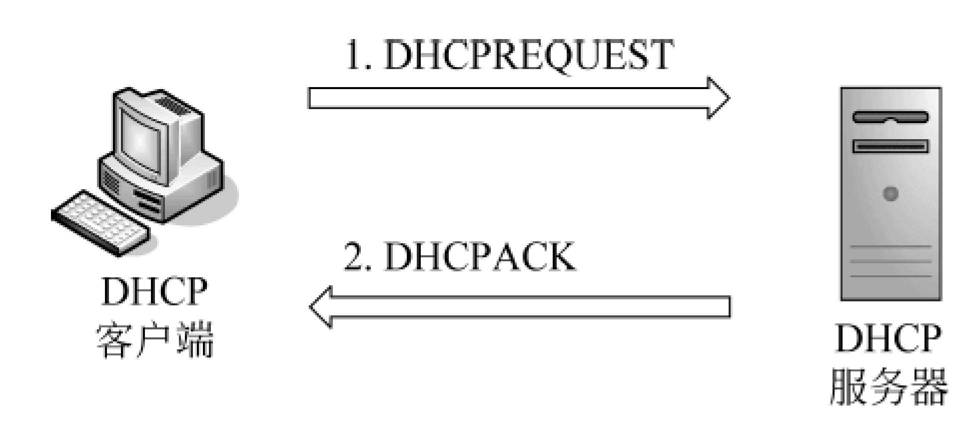


图 8-3　IP 地址的更新与释放

当 IP 租约期过一半时，如果 DHCP 客户端未能从原 DHCP 服务器更新它的 IP 地址租约期，则当租期过 87.5%时，它会以广播的方式向所有的 DHCP 服务器发送 DHCPREQUEST 消息。任一个 DHCP 服务器可以回应 DHCPACK 消息(更新租期)或 DHCPNACK 消息(强制 DCHP 客户端重新初始化并租用新的 IP 地址)。

如果租期已满，DHCP 客户端没有更新租约成功，必须立即停止使用该 IP 地址，并重新进入初始化状态，重新开始 DHCP 租用过程以租用另一个 IP 地址。

3. 自动分配私有 IP 地址

若 DHCP 客户端计算机由于种种原因，无法从 DHCP 服务器租用到 IP 地址时，例如，网络中没有 DHCP 服务器，或是 DHCP 服务器地址池内的地址耗尽，此时这些客户端计算机将会被自动分配一个 Network ID 为 169.254.0.0 的保留 IP 地址。分配到此类 IP 地址的计算机可以临时通信。

客户端计算机使用私有 IP 地址期间，仍然会每隔 5min 来尝试寻找可用的 DHCP 服务器，一旦成功从 DHCP 服务器获取到一个有效的 IP 地址，客户端就会放弃使用的私有 IP 地址。

在命令提示符下，执行 ipconfig 命令，可以查看获取到的私有 IP 地址，如图 8-4 所示。

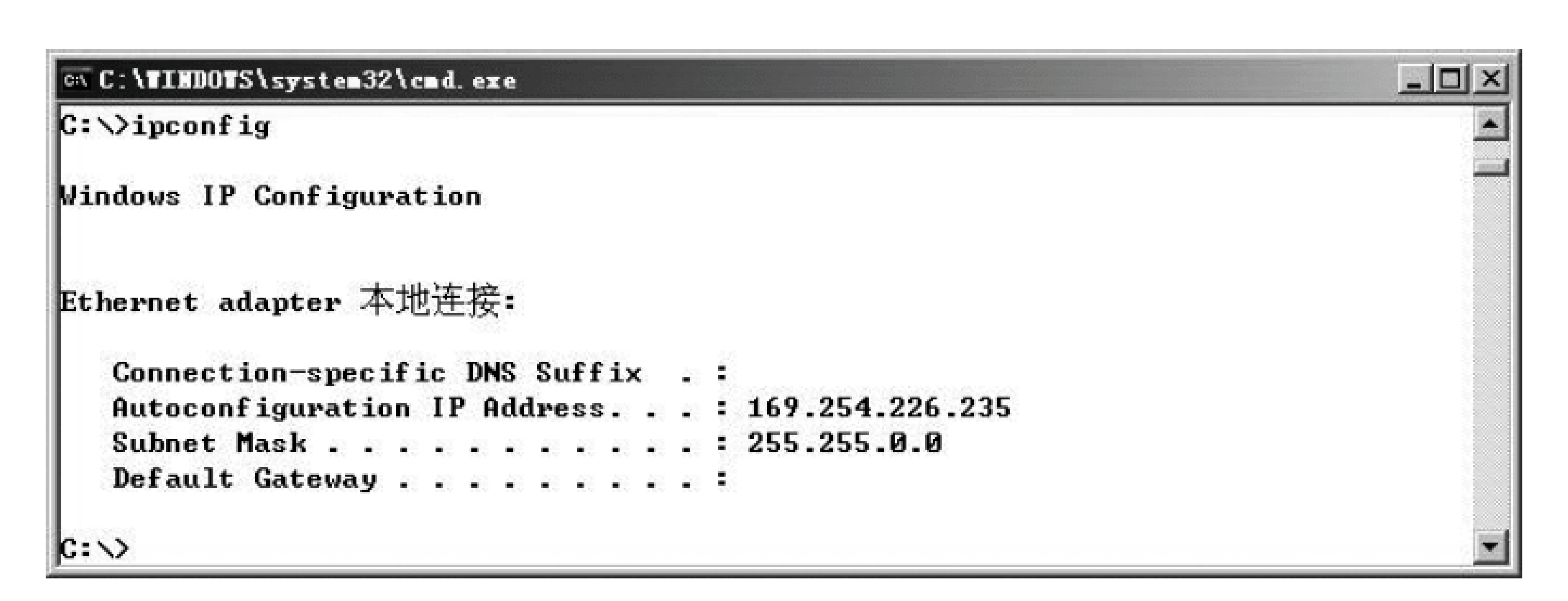


图 8-4　自动私有 IP 地址

8.3 安装 DHCP 服务器

在 Windows Server 2003 上安装 DHCP 服务器之前,需满足以下要求。

(1) 该服务器本身已配置固定的 IP 地址、子网掩码和默认网关。

(2) 具有可用的地址池,即可出租给客户端计算机使用的 IP 地址范围。

要开始安装 DHCP 服务器组件,操作步骤如下。

(1) 单击"开始"→"控制面板"→"添加或删除程序"→"添加或删除 Windows 组件"→选中"网络服务"→单击"详细信息"。

(2) 在图 8-5 中,选择"动态主机配置协议(DHCP)",单击"确定"按钮。

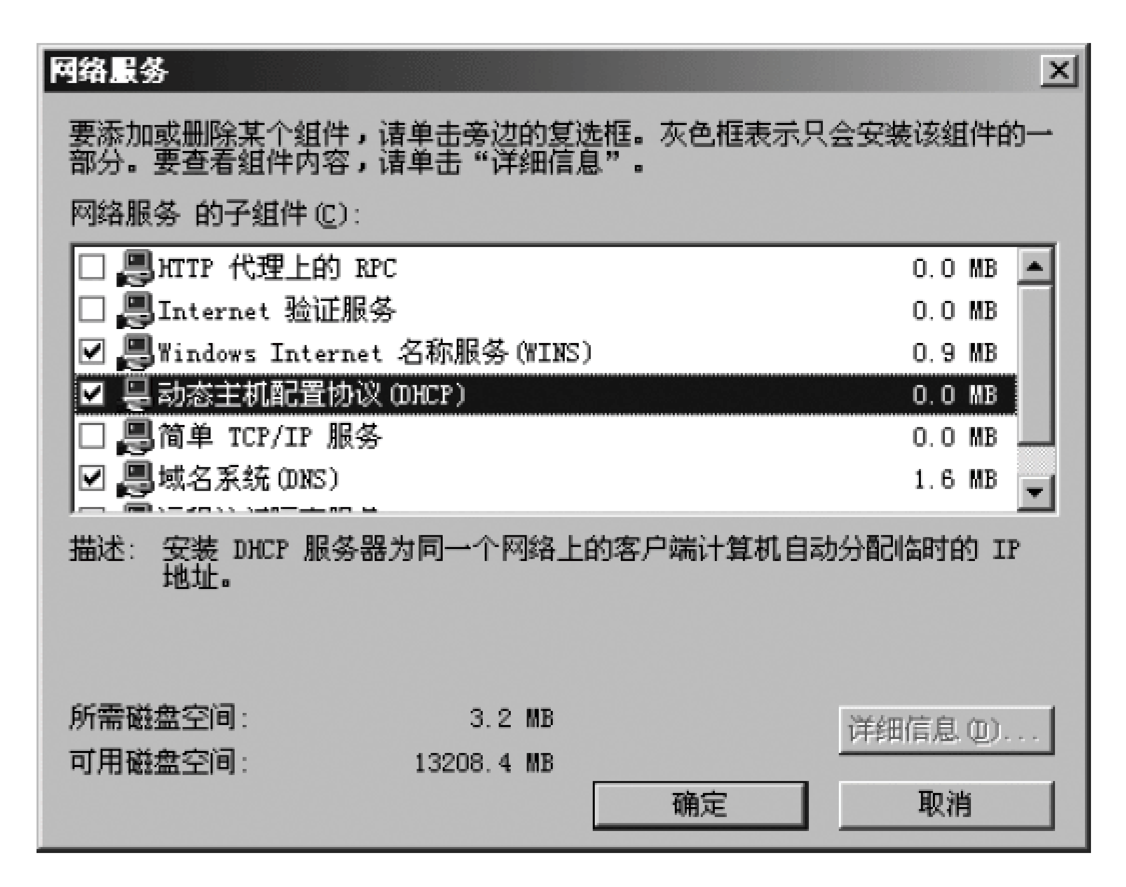


图 8-5 添加动态主机配置协议(DHCP)组件

(3) 返回前一个对话框时,单击"下一步"按钮。安装过程中,可能需要插入 Windows Server 2003 安装盘。

8.4 新建、管理作用域

8.4.1 作用域概述

安装好 DHCP 服务器以后,还不能立即对客户端计算机提供 IP 地址出租服务,只有新建了作用域后,才可以提供分配 IP 地址的服务。

作用域主要保存了指派给 DHCP 客户端的 IP 地址范围,即 IP 地址池。作用域主要包含下列信息。

(1) IP 地址的范围,可在其中加入或排除可用于租用的 IP 地址。

(2) 子网掩码,用于确定 IP 地址所在的子网。

(3) 作用域的名称,在创建作用域时要指派作用域的名称。

(4) 租约期限值,指派给 DHCP 客户端使用 IP 地址的时间。

(5) DHCP 作用域选项,例如 DNS 服务器、路由器和 WINS 服务器的地址等。

(6) 保留,用于确保某个 DHCP 客户端总是能获取到同一个 IP 地址信息。

8.4.2 使用新建作用域向导

要新建作用域,操作步骤为如下。

(1) 在 DHCP 主控制台中,右击 DHCP 服务器,选择“新建作用域”选项。

(2) 在“欢迎使用新建作用域向导”对话框中,单击“下一步”按钮。在图 8-6 中,输入作用域的名称和描述,单击“下一步”按钮。

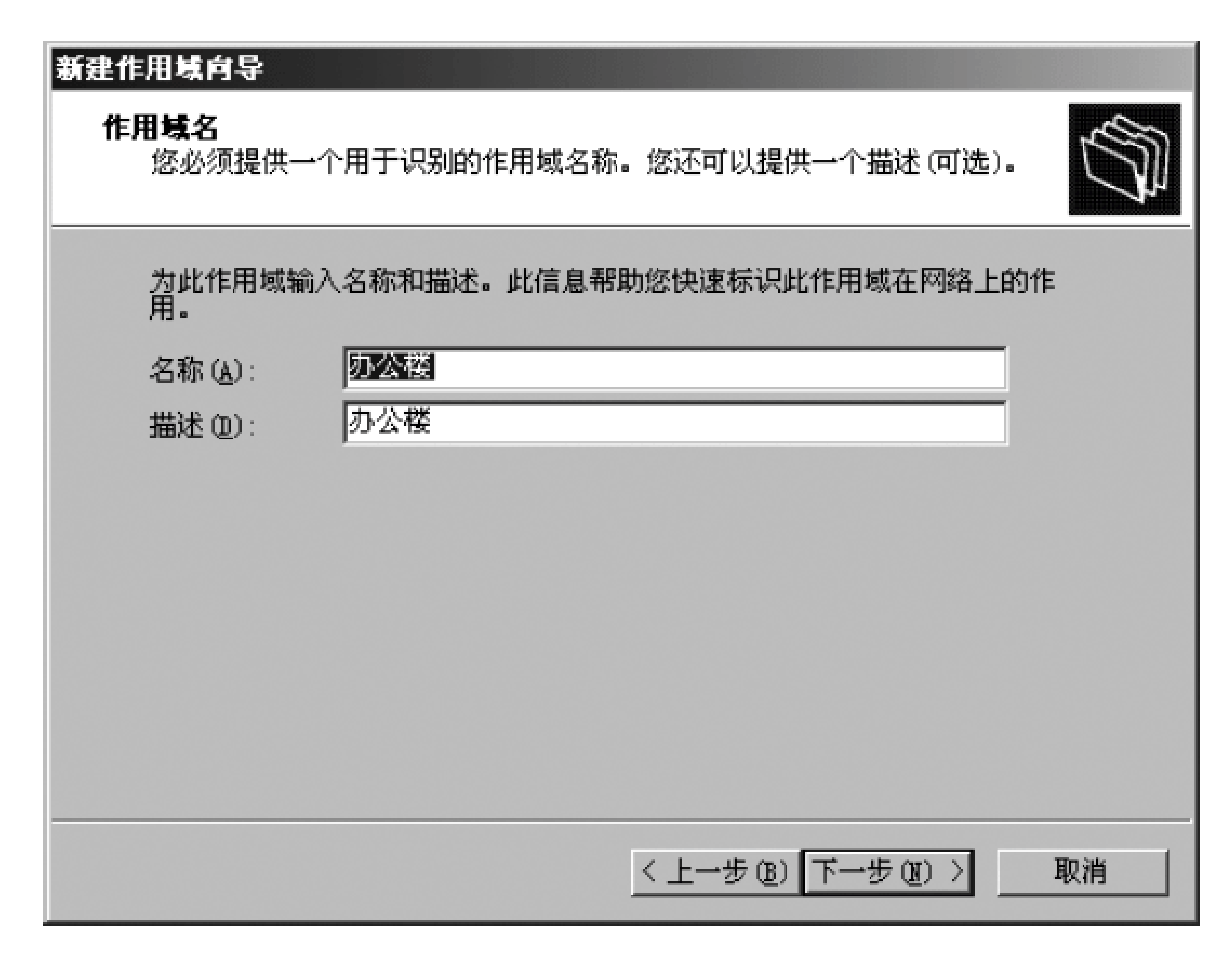


图 8-6　指定作用域名称和描述

(3) 在图 8-7 中,输入可分配的起始 IP 地址与结束 IP 地址,并在“子网掩码”处指定这些 IP 地址的子网掩码,或配置子网掩码的长度,单击“下一步”按钮。

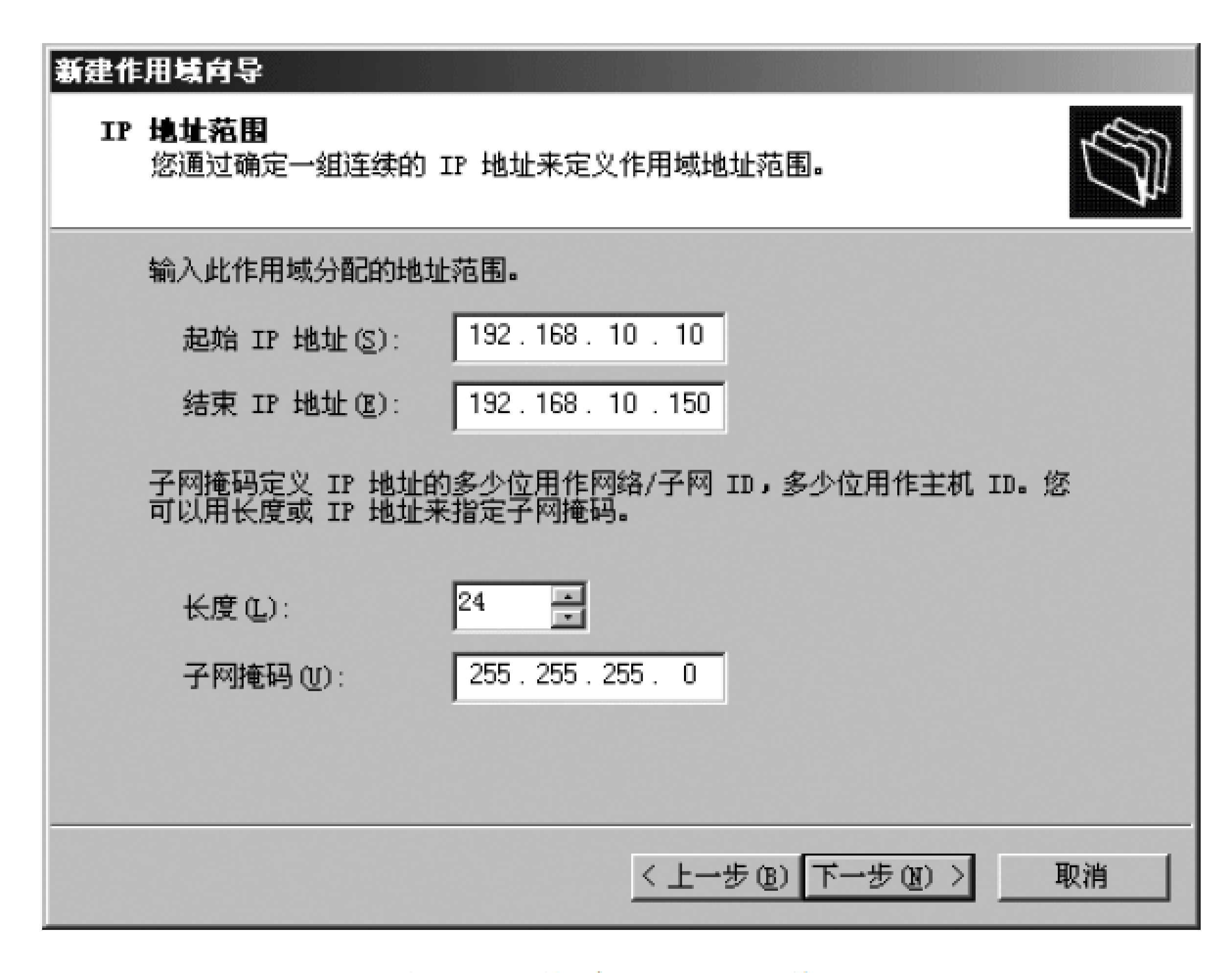


图 8-7　指定 IP 地址范围

（4）在图 8-8 中，可以排除作用域内的一些 IP 地址，设置好后单击“下一步”按钮。

新建作用域向导

添加排除

排除是指服务器不分配的地址或地址范围。

键入您想要排除的 IP 地址范围。如果您想排除一个单独的地址，则只在“起始 IP 地址”输入地址。

起始 IP 地址(S)： 结束 IP 地址(E)：

添加(D)

排除的地址范围(C)：

192.168.10.100 到 192.168.10.110

删除(V)

< 上一步(B) 下一步(N) > 取消

图 8-8　添加排除

（5）在图 8-9 中，设置租约期限，默认为 8 天，设置好后单击“下一步”按钮。

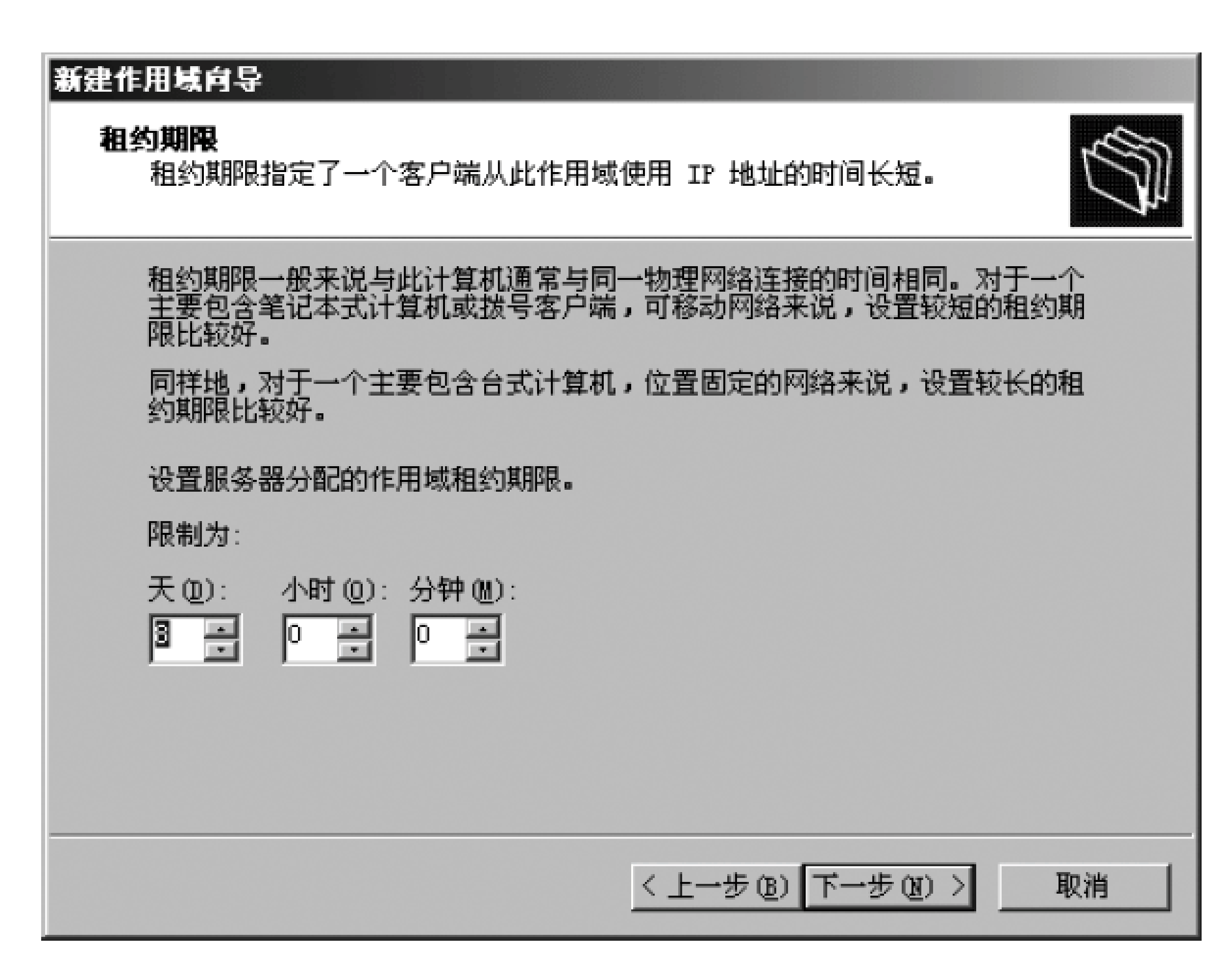


图 8-9　设置租约期限

（6）在图 8-10 中，选中“是，我想现在配置这些选项”单选按钮后，可以配置最常用的 DHCP 选项，例如网关、DNS 服务器和 WINS 服务器等。在此暂不配置 DHCP 配置选项，因此选中“否，我想稍后配置这些选项”单选按钮，单击“下一步”按钮。

（7）出现“完成建立作用域向导”对话框时，单击“完成”按钮。

新建作用域后，需要激活，否则是不能接受 DHCP 客户端的请求的。要激活作用域，操作步骤为：右击该作用域，在弹出的快捷菜单中选择“激活”选项即可，如图 8-11 所示。

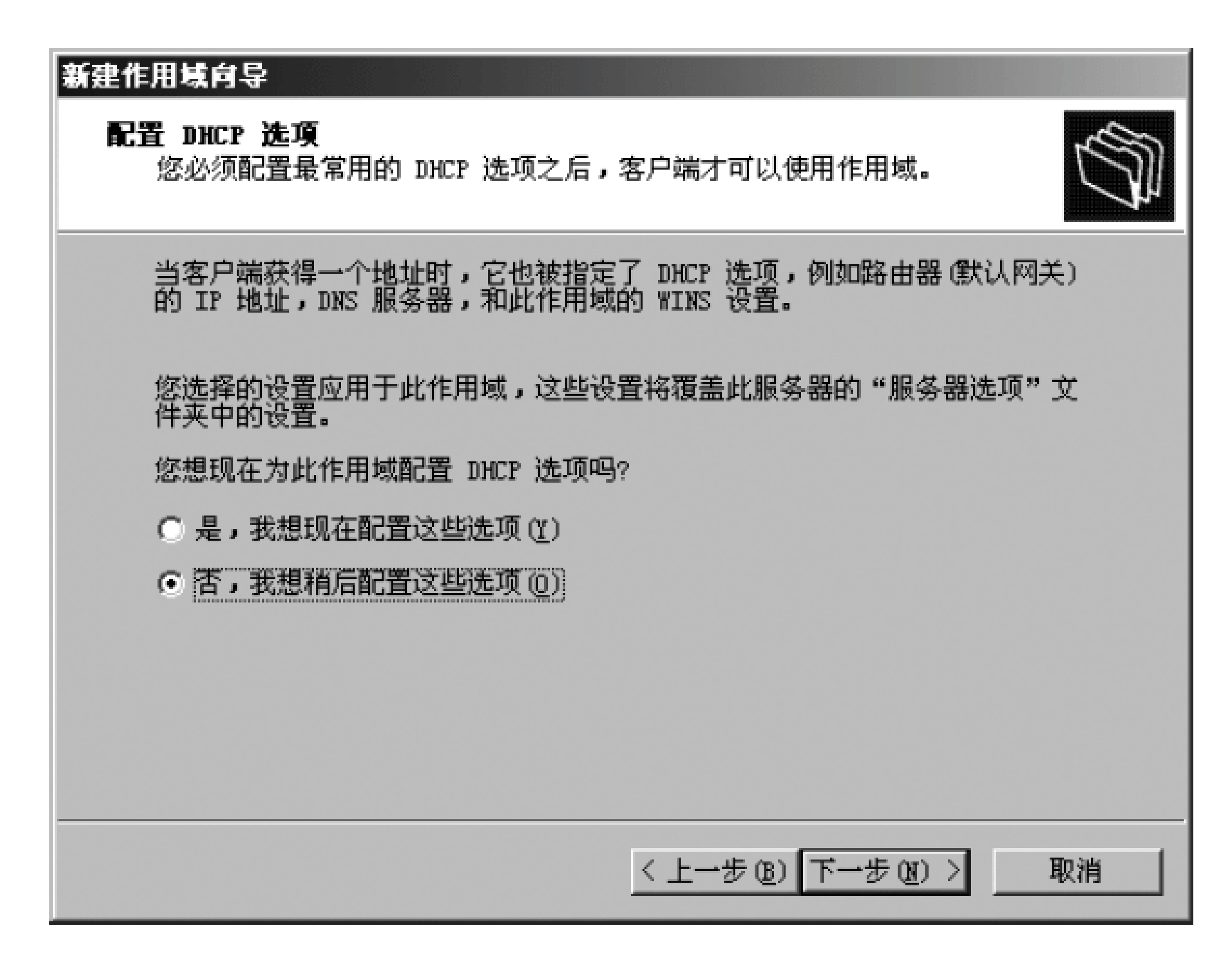


图 8-10　配置 DHCP 选项



图 8-11　激活 DHCP 作用域

8.4.3　配置作用域选项

Windows Server 2003 的 DHCP 服务器提供相当多的配置选项。如果 DHCP 客户端是 Microsoft 操作系统，只有部分的配置选项适用于这些操作系统，例如路由器、DNS 服务器、DNS 区域名称、WINS 服务器、WINS 节点类型等选项。在 DHCP 服务器中可以配置不同级别的 DHCP 选项，这些选项的优先级不同，作用范围也不同，具体来说如下。

(1) 服务器选项。针对该服务器内所有的作用域所配置的选项。

(2) 作用域选项。针对某个作用域所配置的选项。

(3) 保留。针对某个保留 IP 地址所配置的选项。如果没有配置保留的配置选项，保留 IP 将会继承所在作用域选项的配置。

(4) 类别选项。在服务器、作用域、保留内，针对某些特定类别的计算机配置的选项。

当服务器选项、作用域选项、保留选项与类别选项内的配置有冲突时，其优先级为：

服务器选项(最低)→作用域选项→保留选项→类别选项(最高)。

以配置“作用域选项”中的路由器为例,配置选项的操作步骤如下。

(1) 在 DHCP 控制台中,打开作用域,右击“作用域选项”,选择“配置选项”,如图 8-12 所示。



图 8-12　配置作用域选项

(2) 在图 8-13 中,在“可用选项”下选择“003 路由器”,然后在“IP 地址”处输入路由器的 IP 地址,单击“添加”按钮,再单击“确定”按钮。

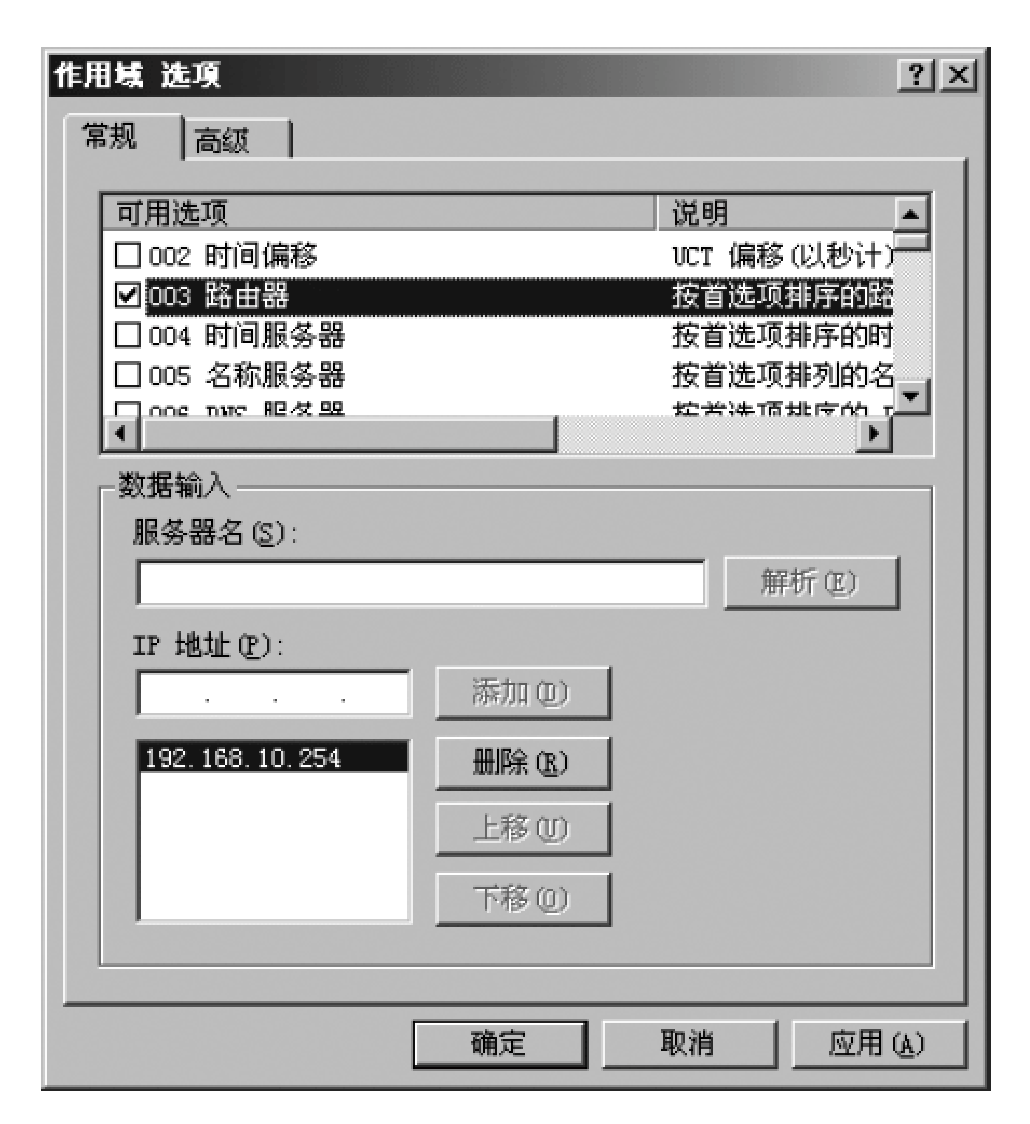


图 8-13　指定路由器选项

配置完成后,如图 8-14 所示。

在 DHCP 客户端的命令提示符下,执行 ipconfig /renew 命令,更新 IP 地址租约,然后执行 ipconfig /all 命令来查看,会发现 DHCP 客户端的路由器已被指定为 192.168.10.254,如图 8-15 所示。



图 8-14 路由器选项

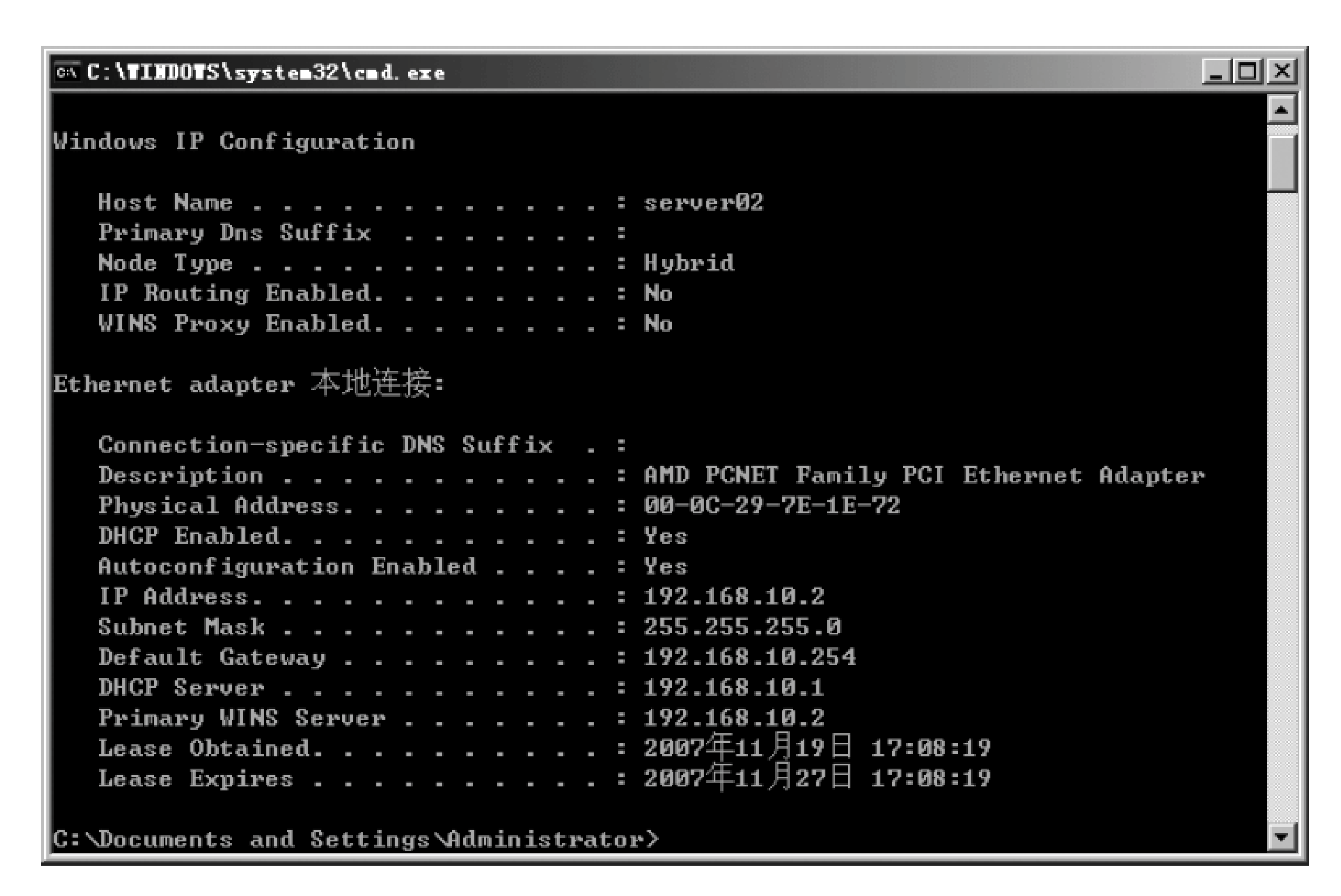


图 8-15 查看 DHCP 客户端信息

8.4.4 IP 地址保留

保留地址主要用于为某一客户端保留一个特定的 IP 地址。在设置保留地址时，要知道客户端网卡的 MAC 地址。

要新建一个保留地址，操作步骤如下。

(1) 在 DHCP 控制台中，展开需要设置保留 IP 地址的作用域，右击“保留”，在弹出的快捷菜单中选择“新建保留”选项，如图 8-16 所示。

(2) 在图 8-17 中，输入相关的信息后，单击“添加”按钮，然后单击“关闭”按钮即可。

可以重复以上步骤，在 DHCP 服务器上保留若干个 IP 地址给某些服务器或客户端使用。

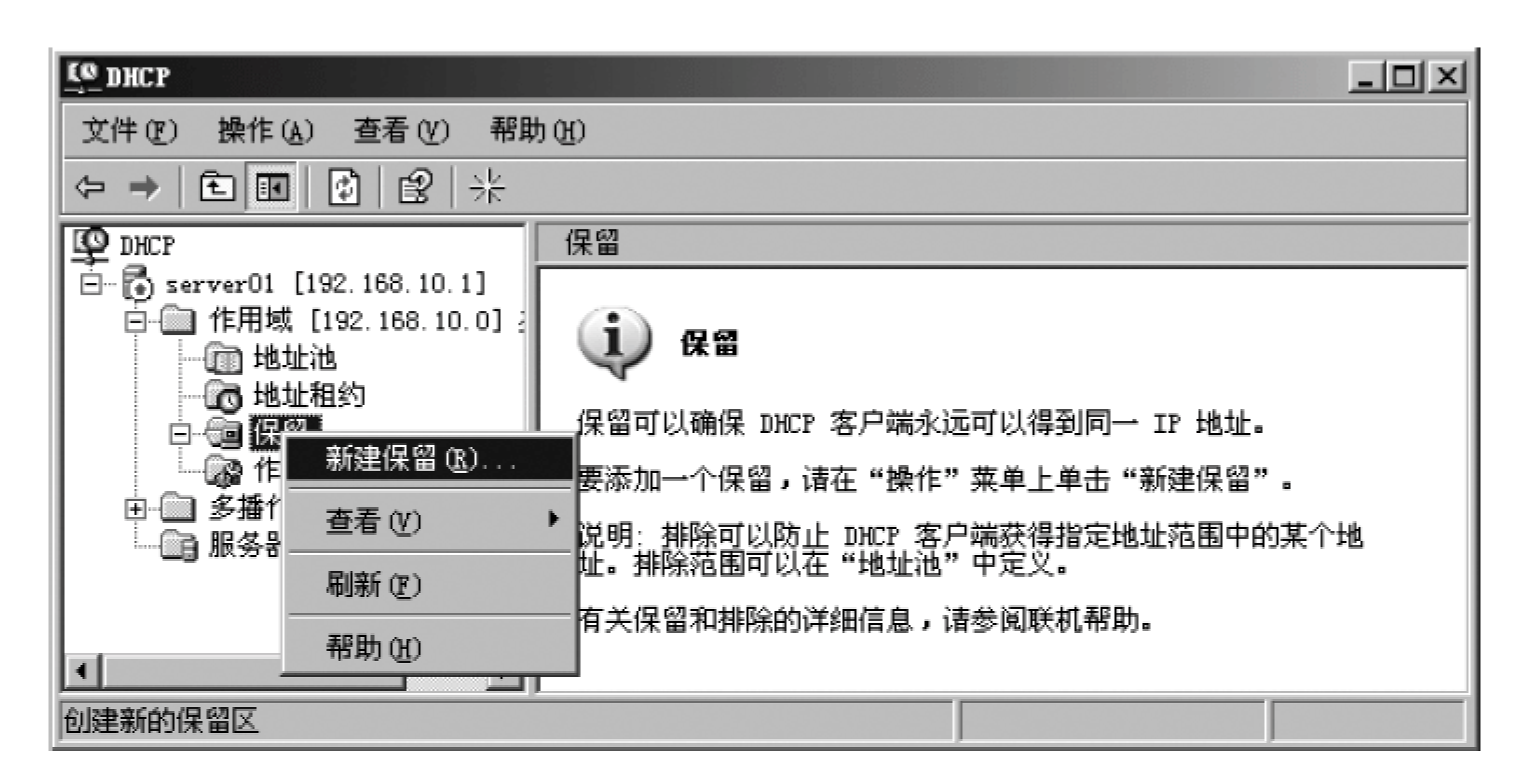


图 8-16　新建保留

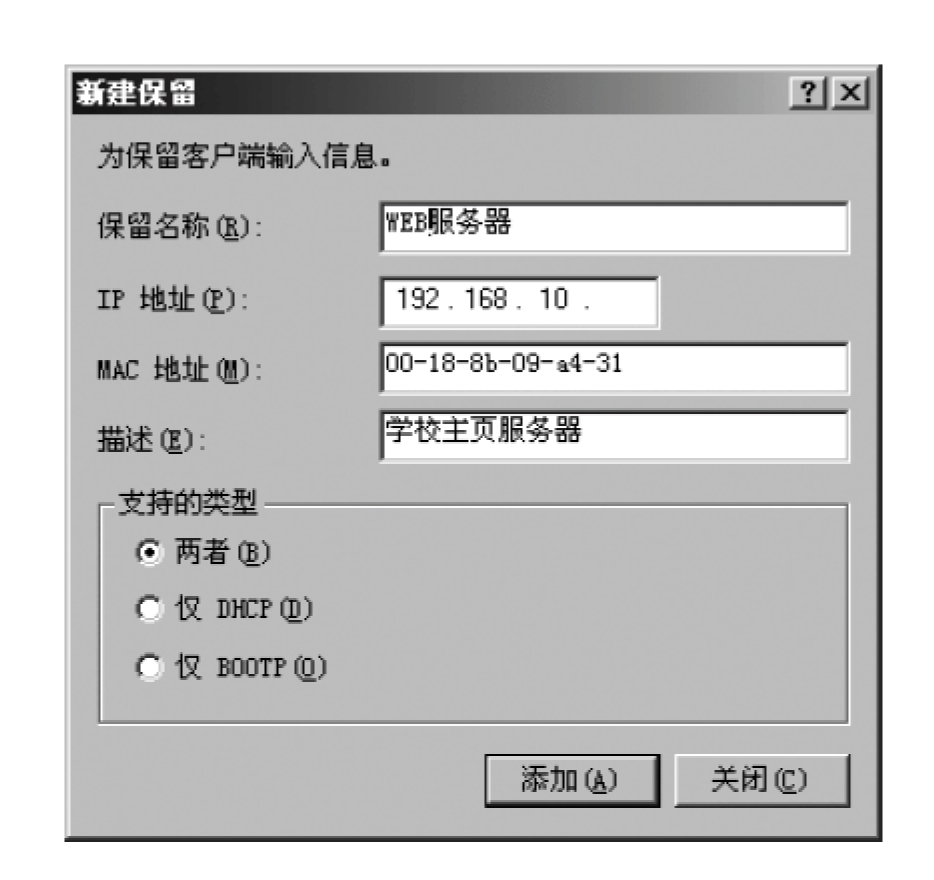


图 8-17　指定保留信息

8.5　配置跨子网 DHCP

一个较大的网络通常会被划分成多个不同的子网，如果 DHCP 服务器和 DHCP 客户端在不同的子网内，因为 DHCP 信息是以广播包的方式传送的，而默认情况下 IP 路由器并不会转发广播信息，因此限制了 DHCP 服务器的使用范围。有 3 种解决此问题的方法。

(1) 在每一个网络中都至少安装一台 DHCP 服务器，使客户端计算机从本网段内的 DHCP 服务器就可以获取 IP 地址信息。

(2) 选择符合 RFC 1542 的 TCP/IP 标准规格的 IP 路由器，以便将 DHCP 信息转发到其他的网段。

(3) 在网络内启用 DHCP 中继代理服务，为局域网中的客户端计算机提供 DHCP 消息中转服务。

8.5.1 跨子网使用 DHCP 的方式

1. 利用符合 RFC 1542 规范的 IP 路由器连接网络

利用符合 RFC 1542 规范的 IP 路由器来转发不同网段的 DHCP 广播信息，实现 DHCP 客户端从 DHCP 服务器获取 IP 地址信息，如图 8-18 所示。

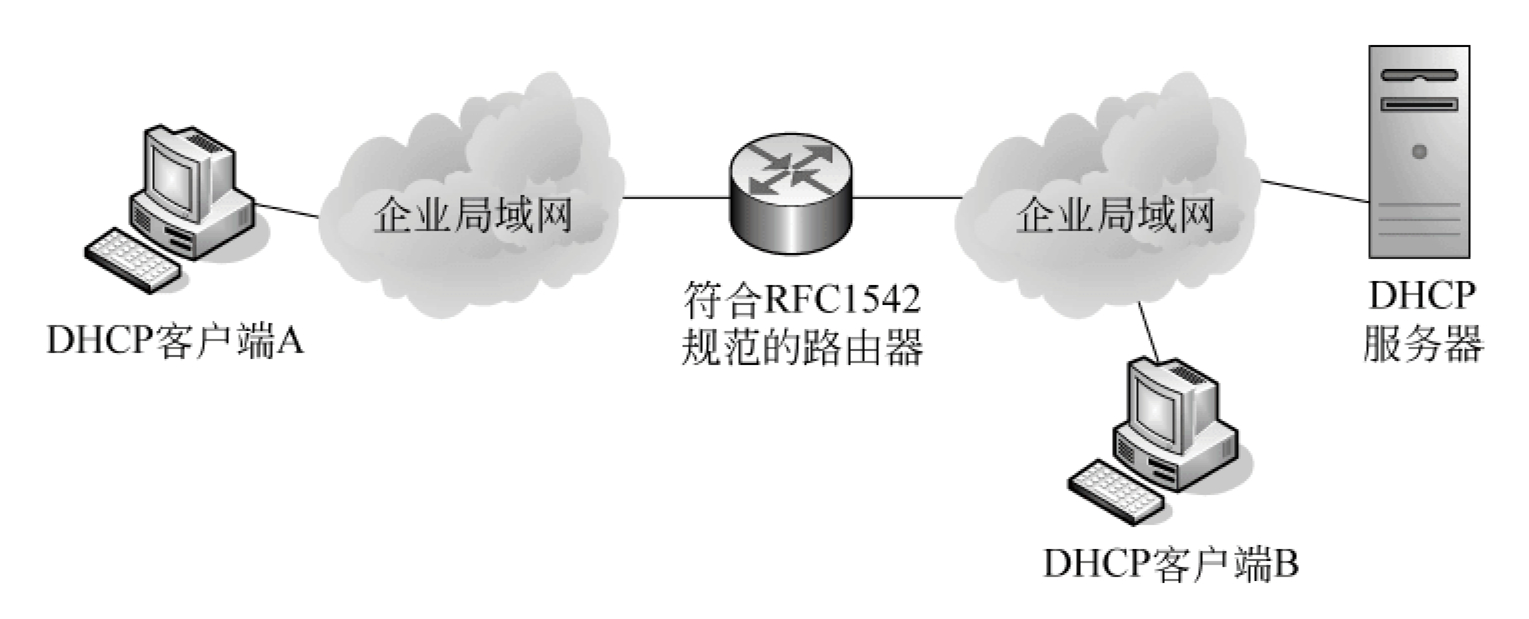


图 8-18 利用符合 RFC 1542 规范的 IP 路由器连接网络

获取 IP 地址的过程如下：

(1) DHCP 客户端 A 发送广播信息 DHCPDISCOVER 来寻找 DHCP 服务器。

(2) 路由器收到此信息后，将此广播信息 DHCPDISCOVER 转发到另一个网段内。

(3) 另一个网段内的 DHCP 服务器收到此信息后，回应 DHCPOFFER 信息给路由器。

(4) 路由器将这个 DHCPOFFER 信息广播给 DHCP 客户端 A。

(5) DHCP 客户端发送 DHCPREQUEST 信息，并经路由器转发给 DHCP 服务器。

(6) DHCP 服务器发送 DHCPACK 信息，并经路由器来转发给 DHCP 客户端。

(7) DHCP 客户端完成从位于不同网段的 DHCP 服务器获取 IP 地址。

2. 用不符合 RFC 1542 规格的 IP 路由器连接网络

如果网络内的 IP 路由器并不符合 RFC 1542 的规格，这时可以在 Windows Server 2003 服务器上启用 DHCP 中继代理，实现 DHCP 客户端从 DHCP 服务器获取 IP 地址信息，因为 DHCP 中继代理也具备将 DHCP 信息转发到其他网段的功能，如图 8-19 所示。

获取 IP 地址的过程如下。

(1) DHCP 客户端 A 利用广播信息 DHCPDISCOVER 寻找 DHCP 服务器。DHCP 中继代理收到此信息后，将其直接转发到另一个网段的 DHCP 服务器。

(2) DHCP 服务器响应信息 DHCPOFFER 给 DHCP 中继代理。DHCP 中继代理将此信息 DHCPOFFER 广播给 DHCP 客户端 A。

(3) DHCP 客户端送出 DHCPREQUEST 信息，DHCP 中继代理收到此信息后，将其直接转发到另一个网段的 DHCP 服务器。

(4) DHCP 服务器送出 DHCPACK 信息，DHCP 中继代理将此信息 DHCPOFFER

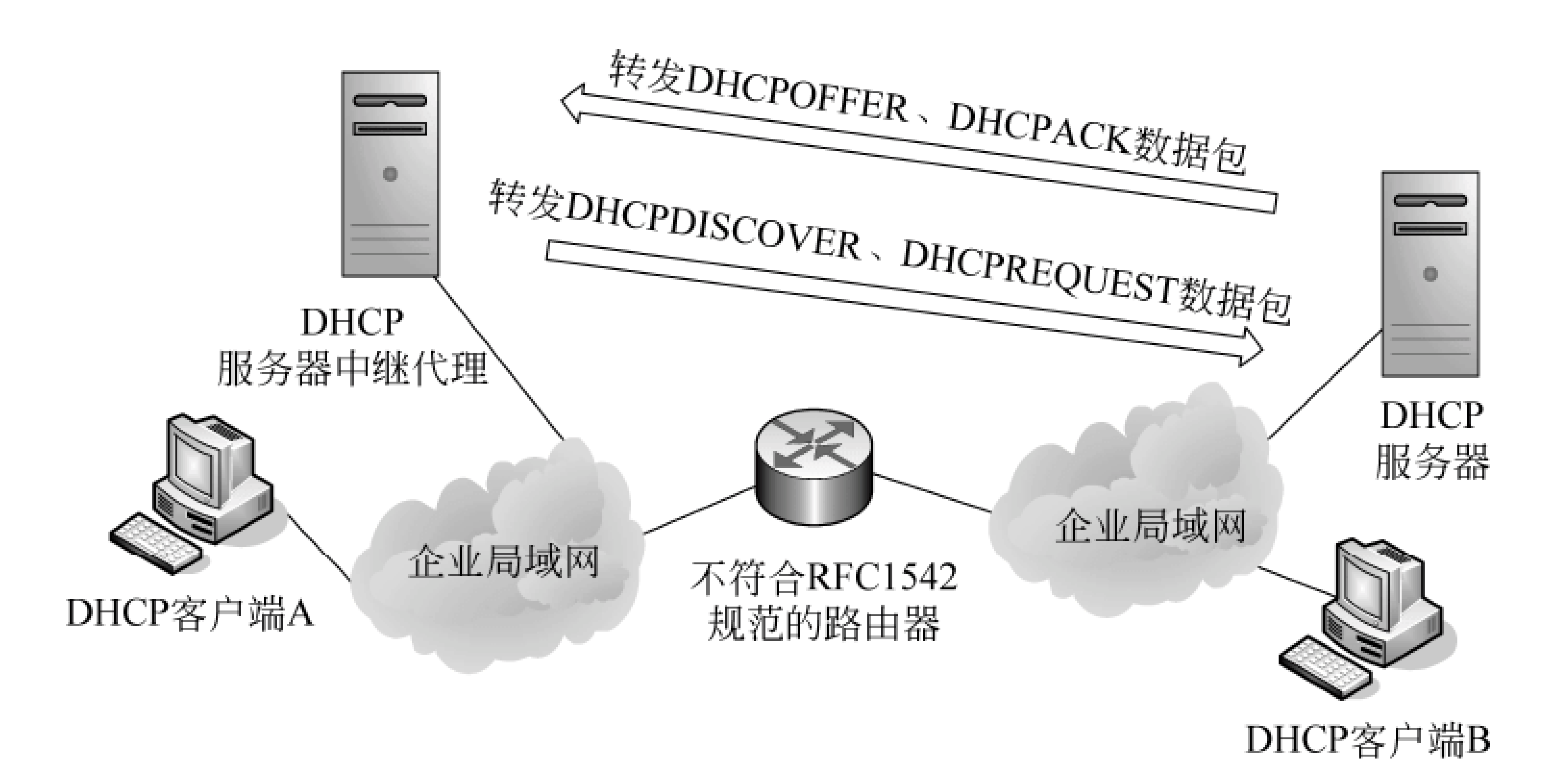


图 8-19 利用不符合 RFC 1542 规格的 IP 路由器连接网络

广播给 DHCP 客户端 A。

(5) DHCP 客户端 A 收到 DHCPACK 信息后,就完成了获取 IP 地址的过程。

8.5.2 配置 DHCP 中继代理

以图 8-20 所示的甲、乙两个网络来举例,要配置乙网络中的 Windows Server 2003 作为 DHCP 中继代理,以便当它收到 DHCP 客户端 B 的 DHCP 信息时,可以将它转发到甲网络的 DHCP 服务器,从而实现乙网络中的 DHCP 客户端 B 能从甲网络中的 DHCP 服务器中获得 IP 地址。

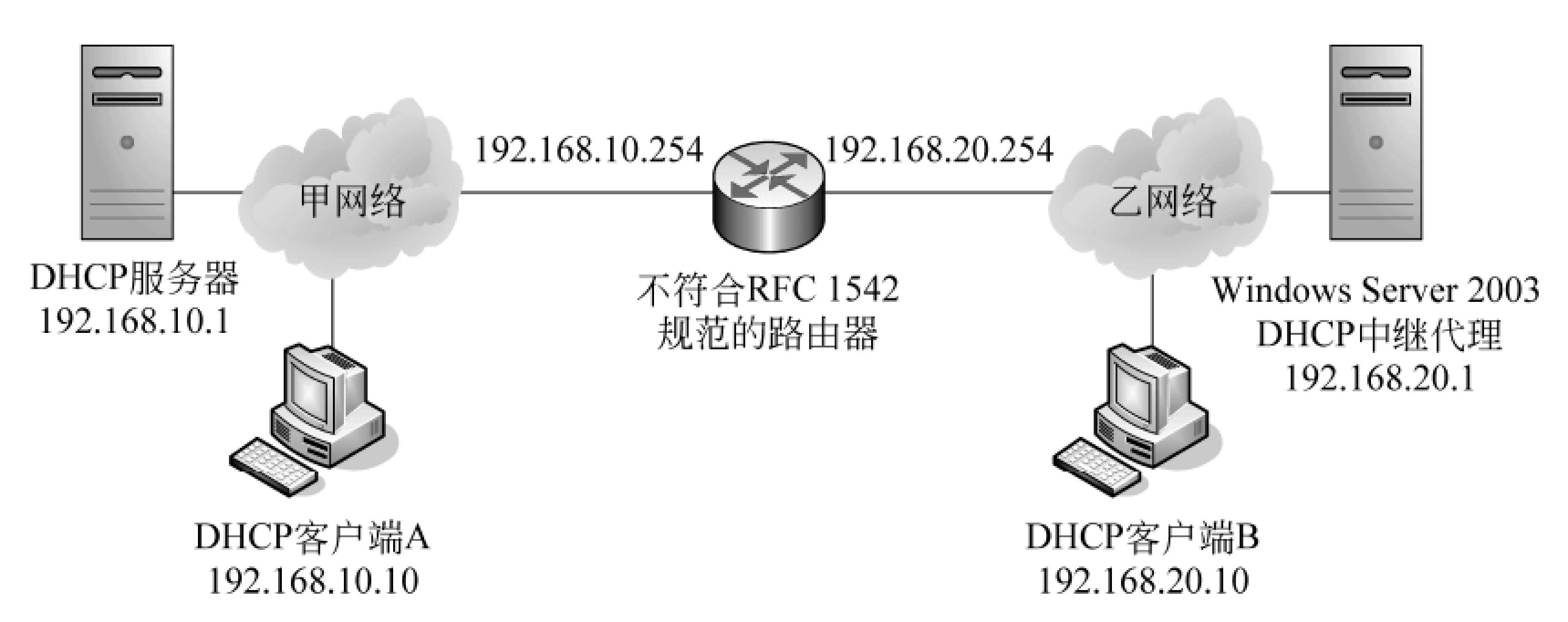


图 8-20 DHCP 中继代理

要配置 DHCP 中继代理服务,操作步骤如下。

(1) 打开"路由和远程访问"控制台,右击服务器,选择"配置并启动路由和远程访问"。

(2) 在"欢迎使用路由和远程访问服务器安装向导"对话框中,单击"下一步"按钮。在图 8-21 中,选择"自定义配置"单选按钮,单击"下一步"按钮。

(3) 在图 8-22 中,选择"LAN 路由"复选框,单击"下一步"按钮。

(4) 出现"完成路由和远程访问服务器安装向导"对话框时,单击"完成"按钮。在

图 8-23 中，单击“是”按钮，即可完成路由和远程访问的安装并初始化。

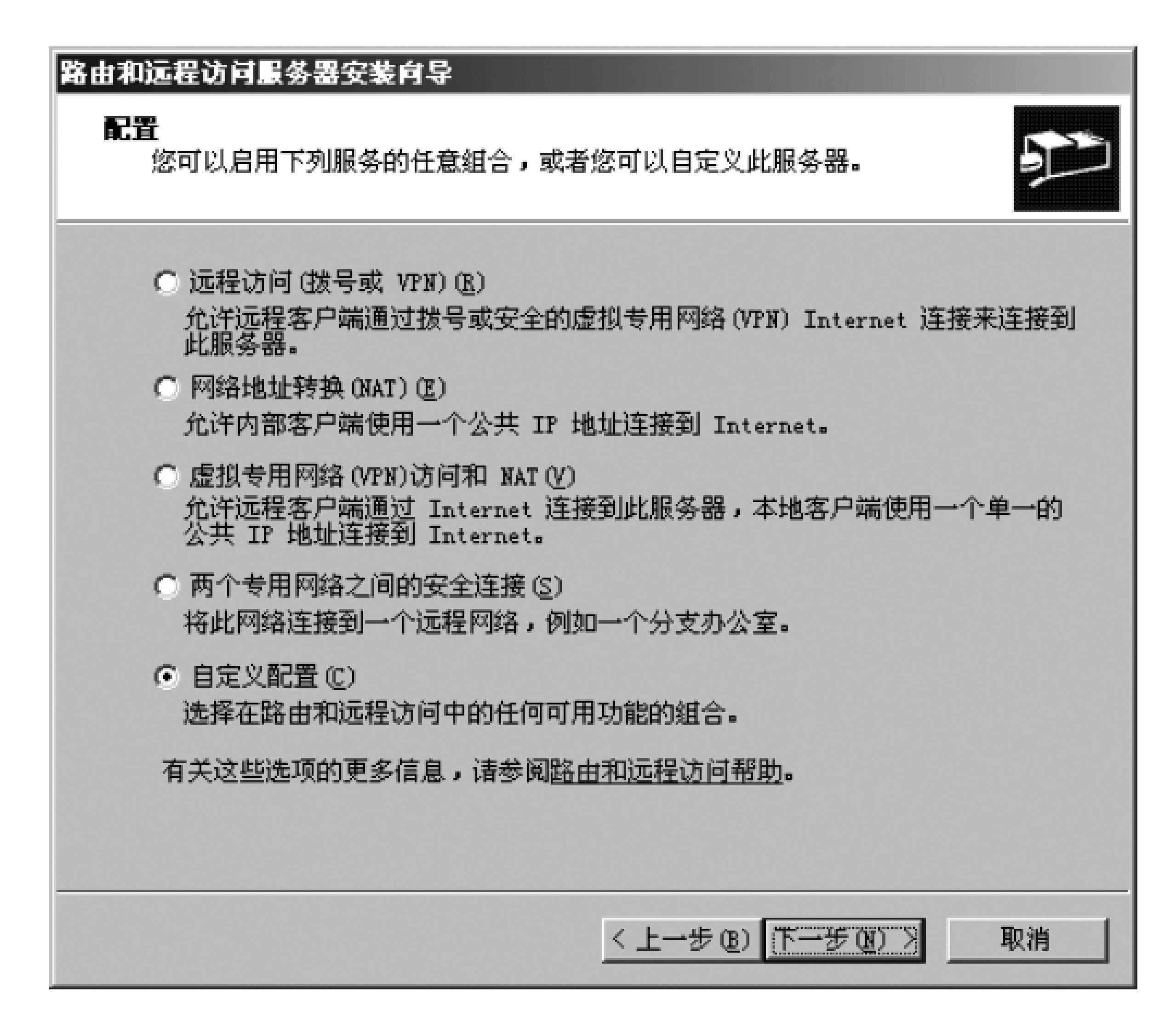


图 8-21　配置路由和远程访问

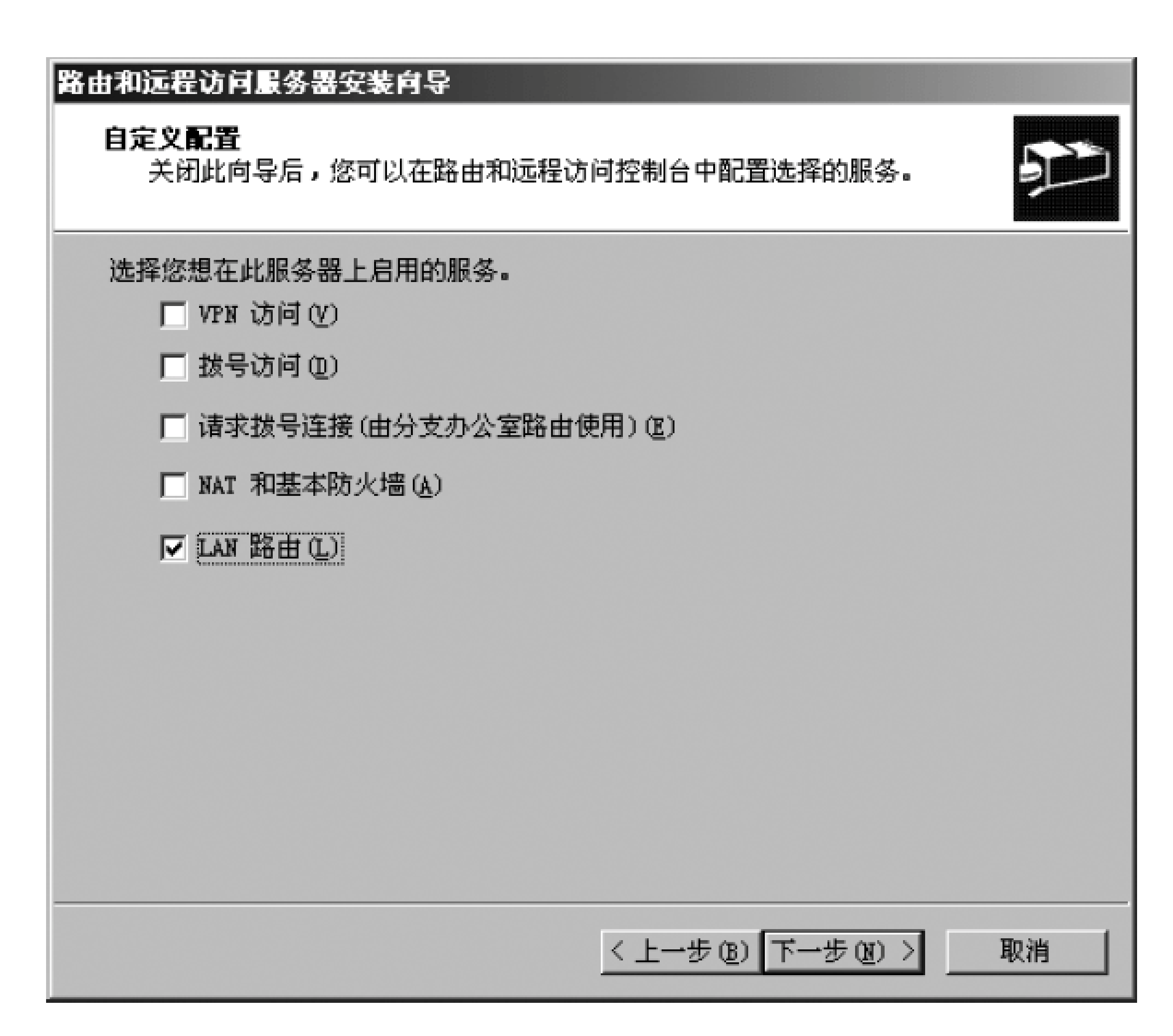


图 8-22　自定义设置



图 8-23　完成路由和远程访问的安装并初始化

要安装 DHCP 中继代理程序，并启用 DHCP 中继代理服务，操作步骤如下。

（1）在“路由和远程访问”控制台中，选择“IP 路由选择”，右击“常规”，选择“新增路由协议”。

（2）在图 8-24 中，选择“DHCP 中继代理程序”，单击“确定”按钮。

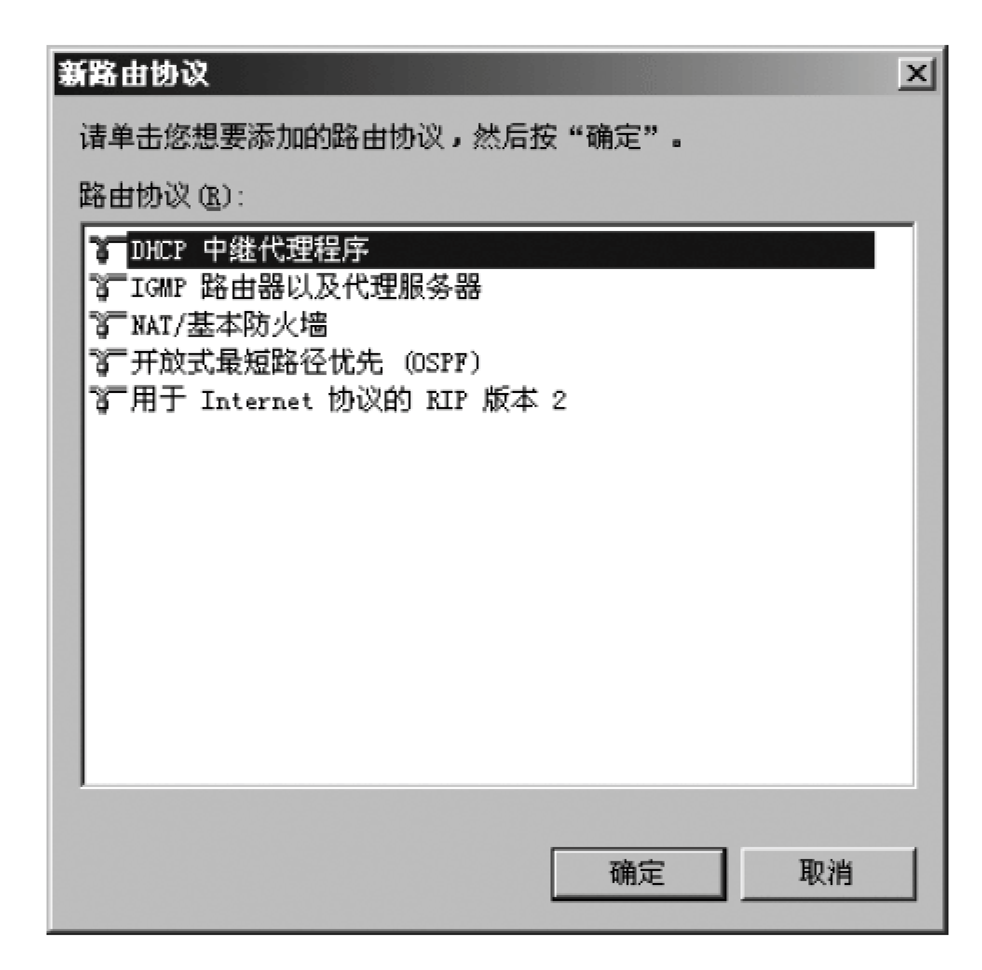


图 8-24　指定新路由协议

（3）安装完 DHCP 中继代理程序后，如图 8-25 所示。

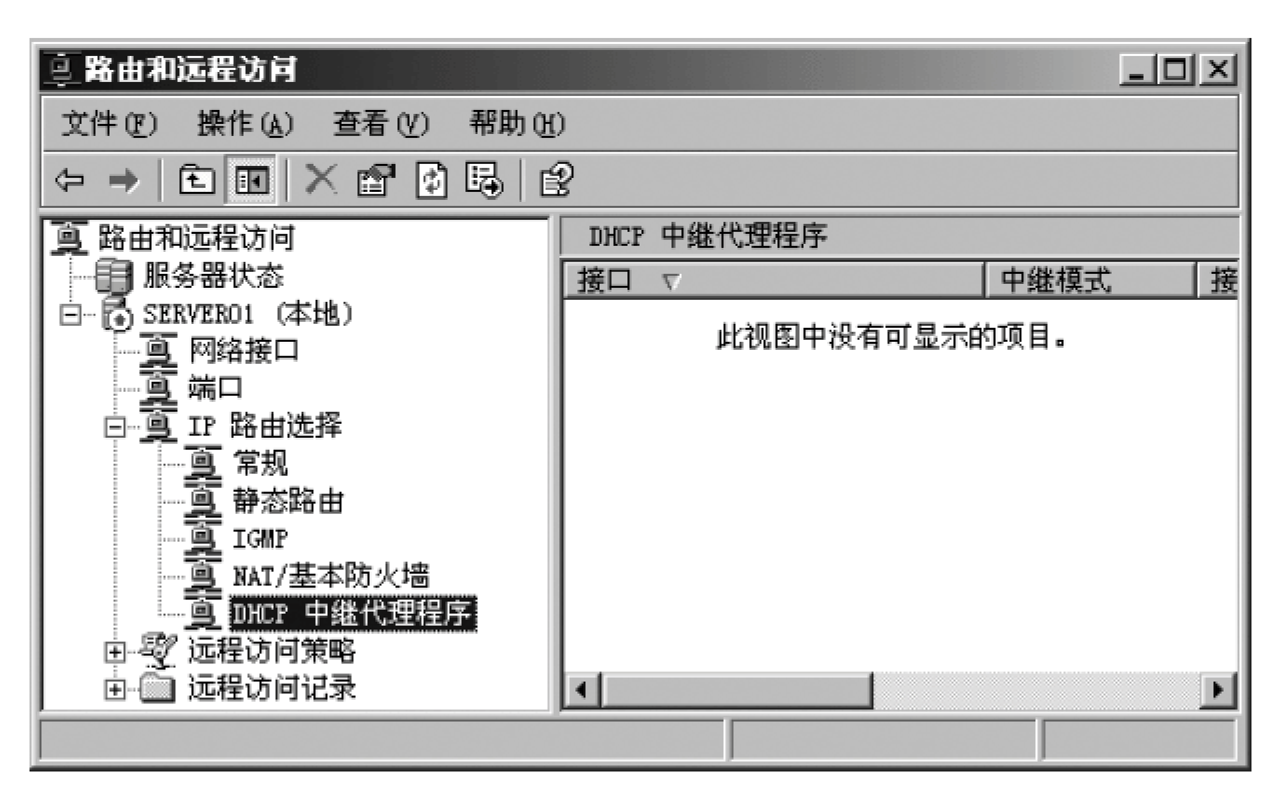


图 8-25　DHCP 中继代理程序

（4）安装完 DHCP 中继代理程序后，还不能立即提供 DHCP 中继代理服务，还要配置将信息转发到一台 DHCP 服务器，并配置转发 DHCP 信息的网络接口。操作步骤为：右击“DHCP 中继代理程序”，在弹出的快捷菜单中选择“属性”选项，如图 8-26 所示。

（5）在图 8-27 中，输入甲网络中 DHCP 服务器的 IP 地址 192.168.10.1，然后单击“添加”按钮和“确定”按钮。

（6）配置转发 DHCP 信息的网络接口，操作步骤为：右击“DHCP 中继代理程序”，在弹出的快捷菜单中选择“新增接口”选项，如图 8-28 所示。



图 8-26　配置 DHCP 中继代理程序

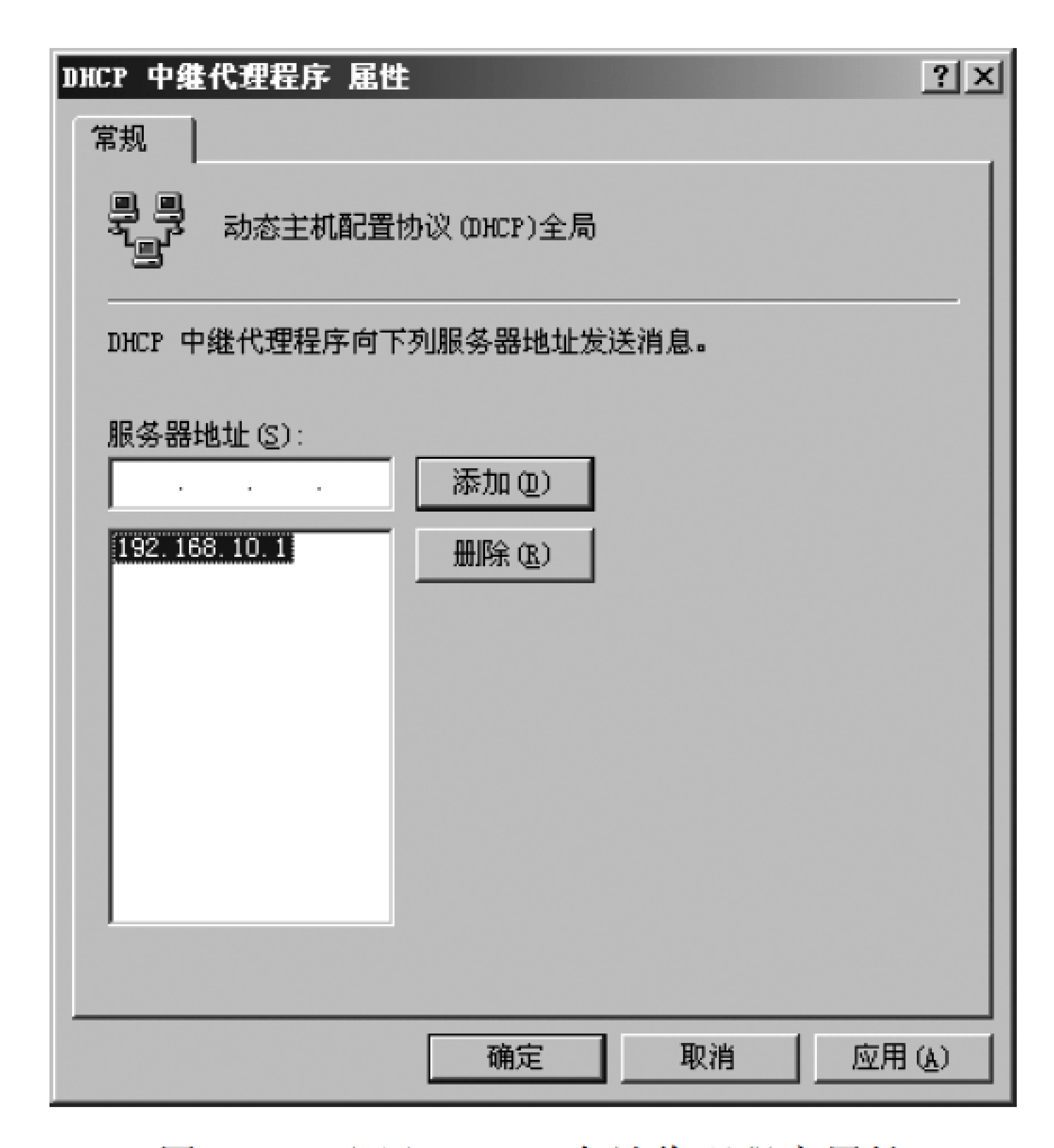


图 8-27　配置 DHCP 中继代理程序属性



图 8-28 新增接口

(7) 选择提供 DHCP 中继代理程序服务的网络接口。

当乙网络中 DHCP 中继代理程序收到通过此接口传送来的 DHCP 信息包时,就会将信息包转发给甲网络中的 DHCP 服务器。未被选择的接口传送过来的 DHCP 信息包,并不会被转发。

如果该服务器内有多个网卡,则会有“本地连接 2”、“本地连接 3”等可供选择。图 8-29 中选择的“本地连接 1”是乙网络中的中继代理服务器的 IP 地址为 192.168.20.1 的网络接口。然后单击“确定”按钮。

(8) 在图 8-30 中,可设置的选项有两个。



图 8-29 指定 DHCP 中继代理程序的接口

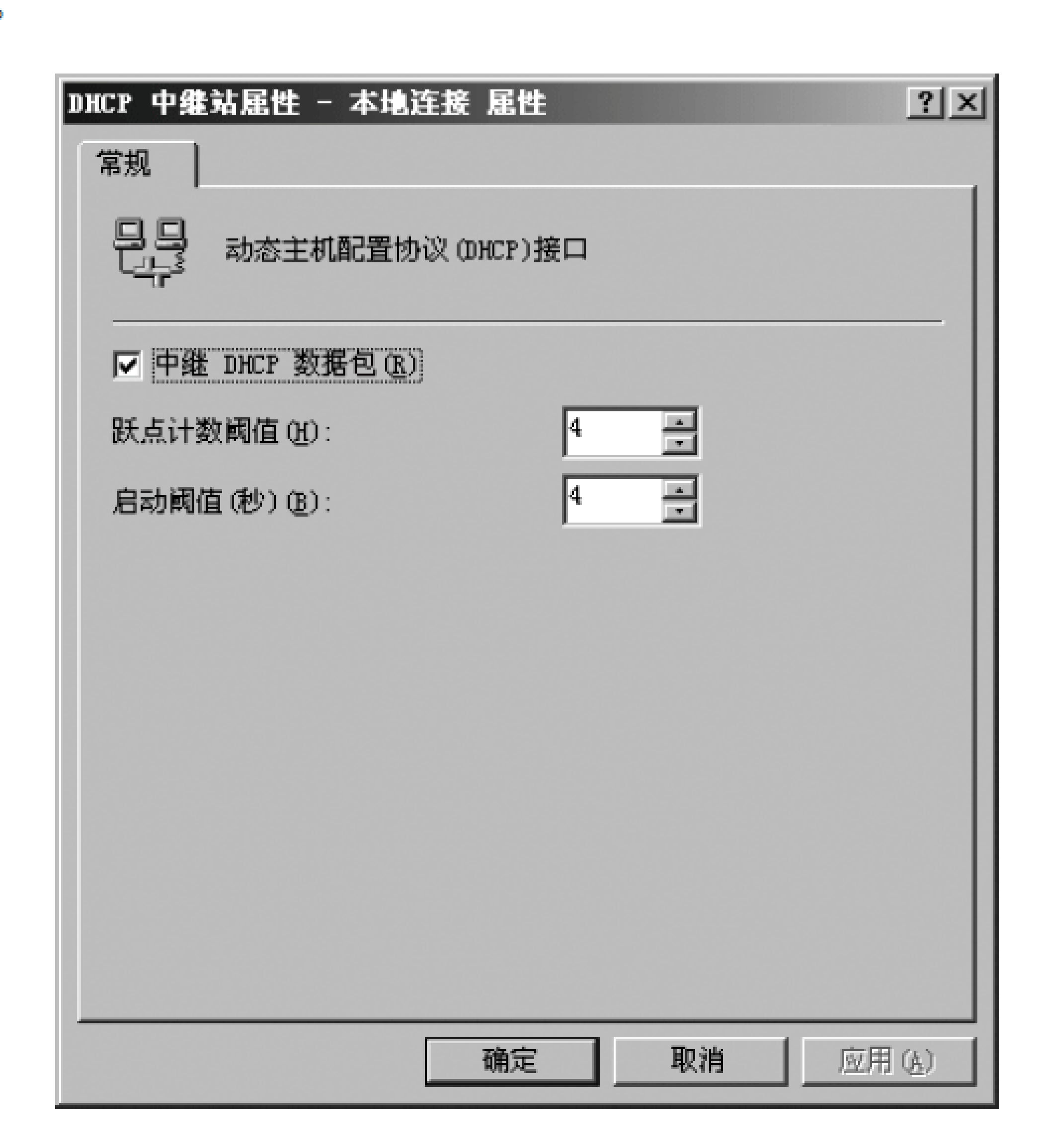


图 8-30 DHCP 中继站属性

① 跃点计数阈值。表示 DHCP 信息最多只能够经过多少跳来转发。

② 启动阈值。在 DHCP 中继代理程序收到 DHCP 信息后，要等此处所配置的时间过后，才会将信息转发给远程的 DHCP 服务器。

一般采用默认设置，单击“确定”按钮，即可完成 DHCP 中继代理的网络转发接口配置。

第 9 章　Web 服务器

学习目标

学习完本章后，了解 IIS 的最新特征，掌握如何安装与测试 IIS，学会如何通过 IIS 发布 Web 网站，掌握虚拟目录的应用，并掌握网站的安全性设置。

9.1　Internet Information Server 概述

Internet Information Server 6.0 已成为 Windows Server 2003 默认的组成部分，IIS 6.0 和以往的版本相比，被重新设计，并取消了传统的配置文件格式 Meta Database，采用了全新的 XML 文件存储格式；与 Windows Server 2003 中其他应用程序服务结合得更加紧密合理；在可靠性、可扩展性、安全性、应用支持和可管理性方面都有了很大提高；还支持其他一些功能强大的组件，包括活动的服务器页面(Active Server Page，ASP)、互联网服务器应用程序接口(Internet Server Application Programming Interface，ISAPI)、互联网数据连接器(Internet Data Connector，IDC)等；在安全方面有很大改善，例如，默认仅安装显示静态 HTML 页面所需的组件，而不允许动态内容。

9.1.1　客户端访问 Web 服务器的流程

当 Web 服务器接收到客户端计算机的 HTTP 请求后，就会返回一个 HTTP 响应。Web 服务器可以响应一个静态页面或图片，或者页面重定向，或者通过一些其他的程序，例如 CGI 脚本、JSP 脚本、ASP 脚本、服务器端 JavaScript 等。但最终 Web 服务器会返回 HTML 代码给浏览器，再由浏览器负责将其显示给用户。

客户端访问 Web 服务器的流程，大致可分为三步。

(1) 客户端的 Web 浏览器向一个特定的 Web 服务器发出 Web 页面请求。

(2) Web 服务器接收到客户端的 Web 页面请求后，查找所请求的 Web 页面。

(3) Web 服务器将查找到 Web 页面传送给 Web 浏览器，并将它显示出来，如图 9-1 所示。

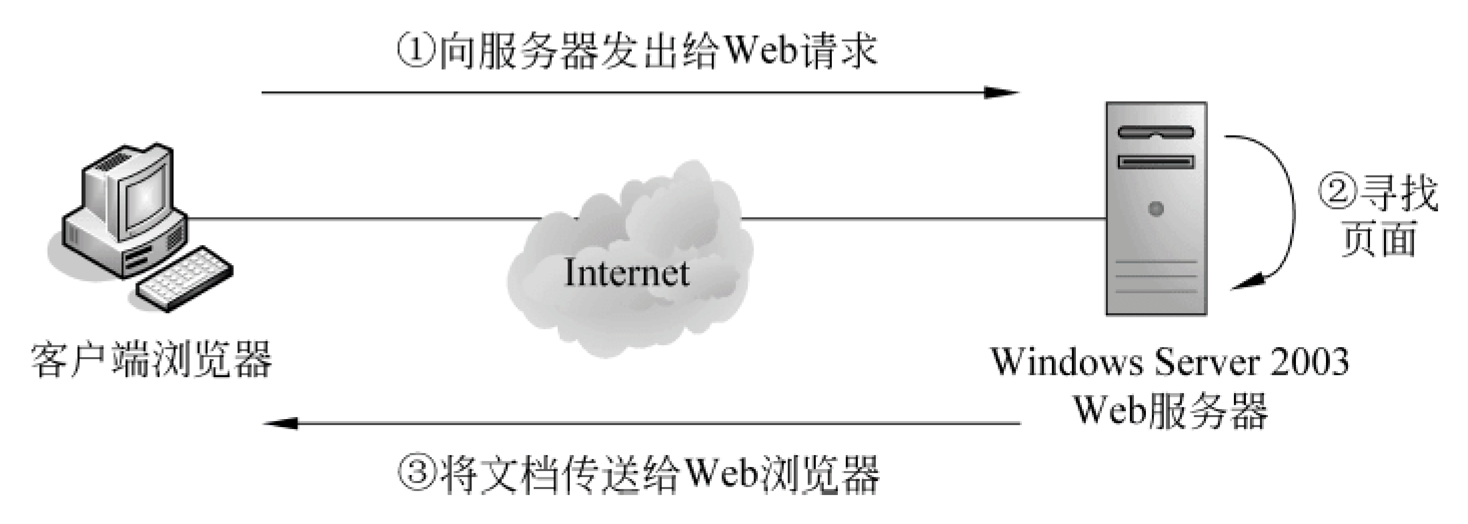


图 9-1　客户端访问 Web 服务器的流程

9.1.2 安装 IIS 组件

安装 IIS 的计算机的 IP 地址最好是固定的，即手工输入 IP 地址、子网掩码、默认网关等信息。若要让用户通过域名来访问此网站，还要在 DNS 服务器上为此服务器分配一个 DNS 主机名，并建立主机名与 IP 地址之间的映射关系。

在 Windows Server 2003 上，安装 IIS 的操作步骤如下。

(1) 单击"开始"→"控制面板"→"添加或删除程序"→"添加/删除 Windows 组件"，选择"应用程序服务器"，单击"详细信息"。

(2) 在图 9-2 中，选中"Internet 信息服务(IIS)"复选框，默认同时会选中"启用网络 COM+访问"，如果要发布.NET 网站，还需选中 ASP.NET。完成后，单击"确定"按钮。

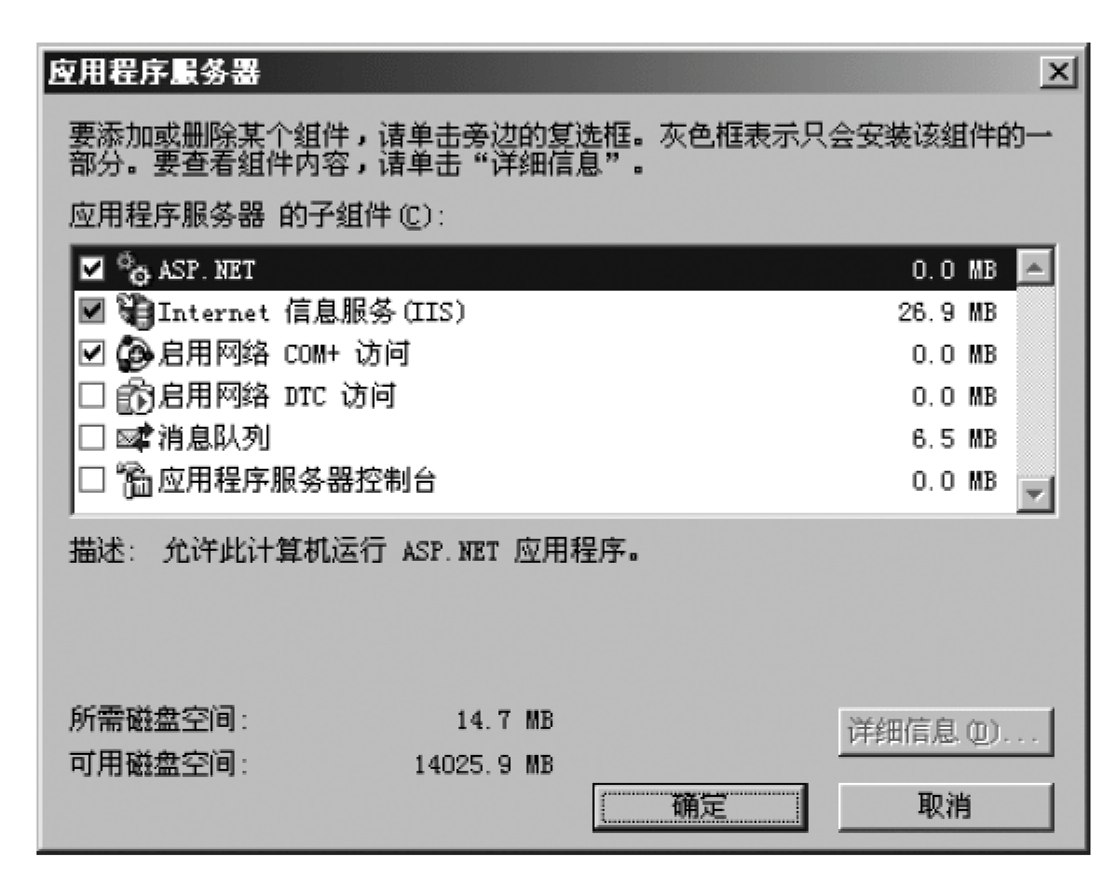


图 9-2 选中安装 IIS 及相关的组件

在 IIS 安装过程中，可能需要插入 Windows Server 2003 安装盘。

完成安装后，打开"Internet 信息服务(IIS)管理器"，即可对 IIS 进行管理。

9.1.3 检查默认安装

假设已安装的 Web 服务器的 IP 地址为 192.168.10.1，计算机名称为 server01，主机头(FQDN)已设置为 www.xyz.net。

要管理网站，打开"Internet 信息服务(IIS)管理器"，如图 9-3 所示。

要连接与测试网站，打开另外一台 Windows 客户端计算机的 IE 浏览器，并在地址栏中输入以下地址。

(1) 利用主机头，输入 http://www.xyz.net。

(2) 利用 IP 地址，输入 http://192.168.10.1/。

(3) 利用计算机名称，输入 http://server01/。

若连接成功，则会出现如图 9-4 所示的界面。



图 9-3 Internet 信息服务(IIS)管理器

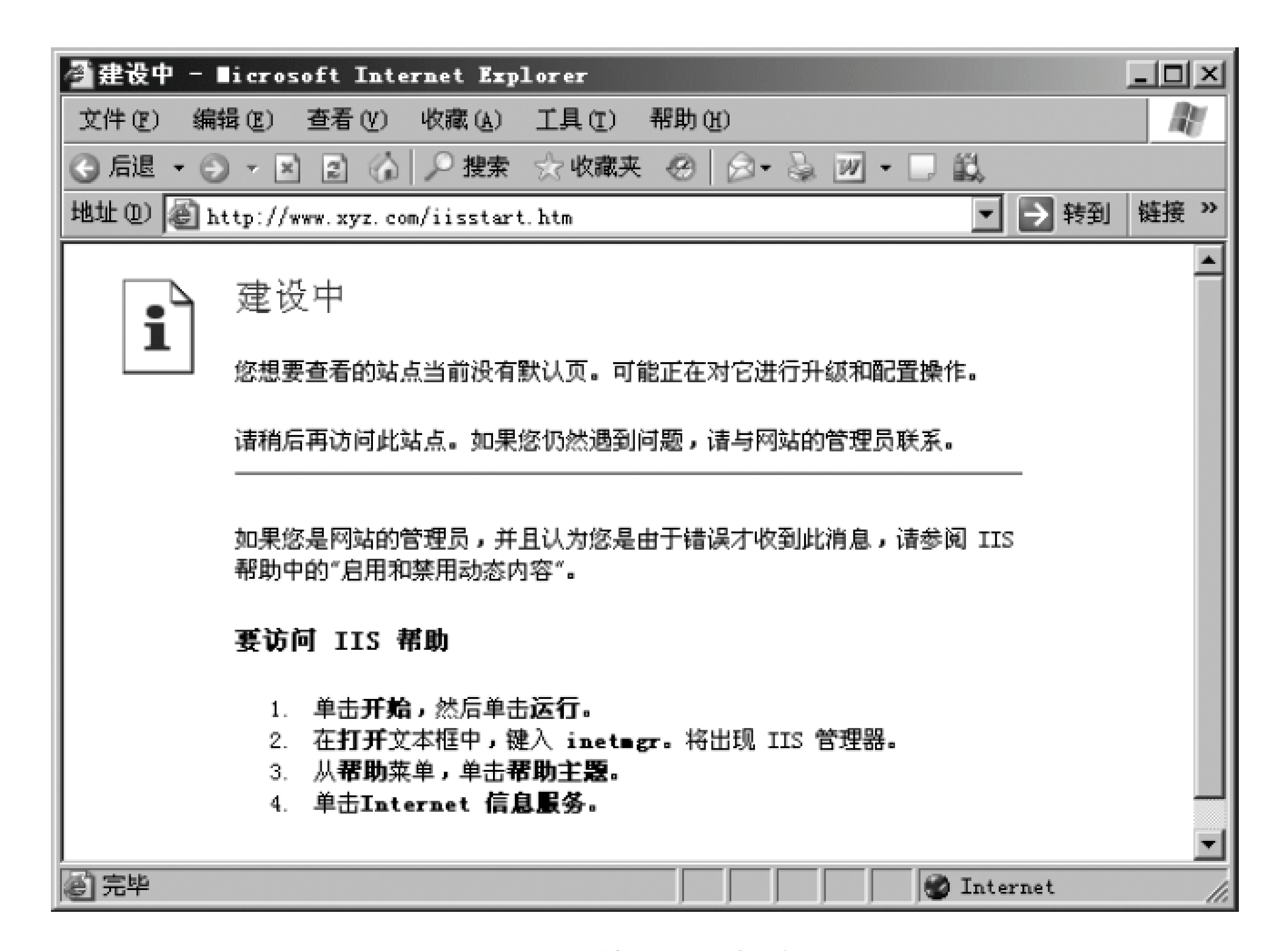


图 9-4 连接测试成功界面

9.2 配置 Web 站点属性

要配置 Web 网站(例如 IIS 内置的“默认网站”)的属性，操作步骤为：右击“默认网站”→选择“属性”→选择“网站”选项卡，可以设置 Web 站点的描述、IP 地址和 TCP 端口号，还可以设置连接超时的时间、日志文件格式和日志属性等，如图 9-5 所示。

1. 主目录设置

选择“主目录”选项卡，可以设置 Web 站点的主目录、目录存取权限、应用程序保护等，如图 9-6 所示。

(1) 此计算机上的目录。默认在%systemdrive%\inetpub\wwwroot 文件夹内，可以修改这个主目录的本地路径。

(2) 另一台计算机上的共享。将主目录指定到另外一台计算机的共享文件夹，该共享文件夹中必须有网页。在“网络目录”中输入“\\服务器名称\共享文件夹名\”格式的

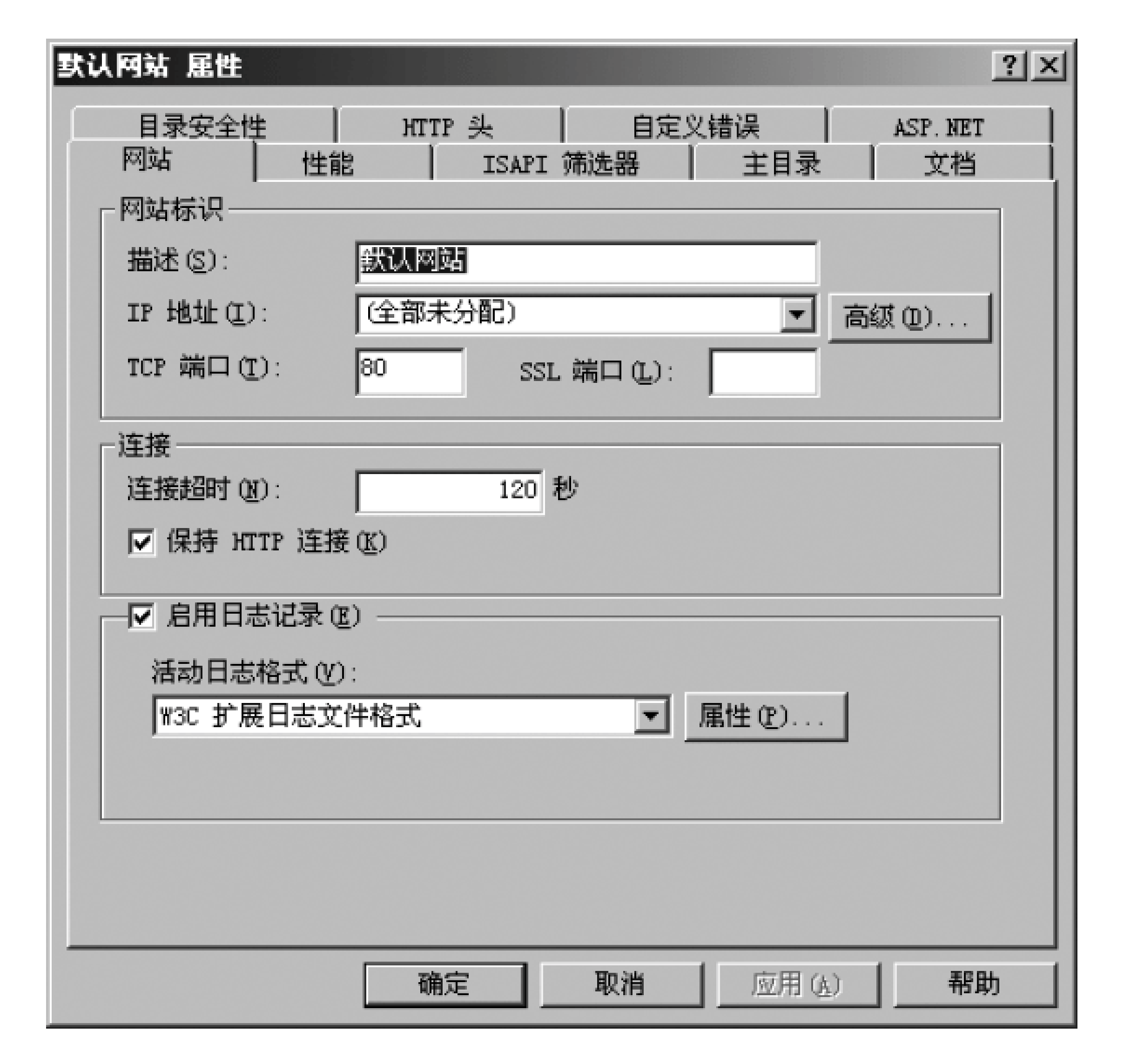


图 9-5　配置“默认网站”属性

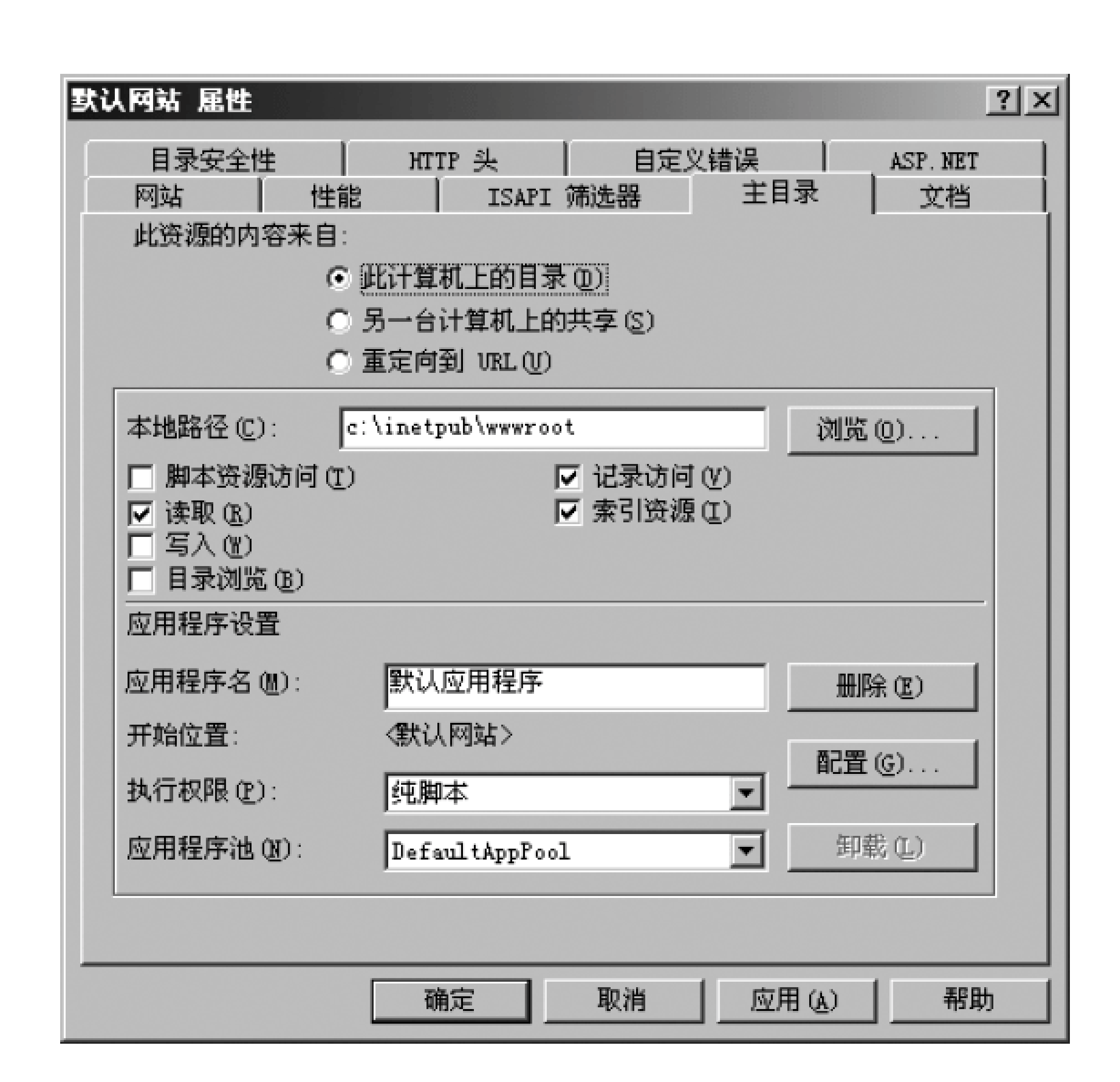


图 9-6　主目录设置

UNC 路径，此时要求该服务器有访问此共享资源的权限。

(3) 重定向到 URL。可以将网站 www.xyz.net 定向到 www.abc.net，当用户访问 www.xyz.net 时，将显示 www.abc.net 网站的内容。

2. 文档设置

在客户端访问某网站时，只需在浏览器的地址栏中输入站点的主机名，并不需要输入主页的文件名，这是因为在该站点的“文档”选项卡中已经指定了主页文件，如图 9-7

所示。

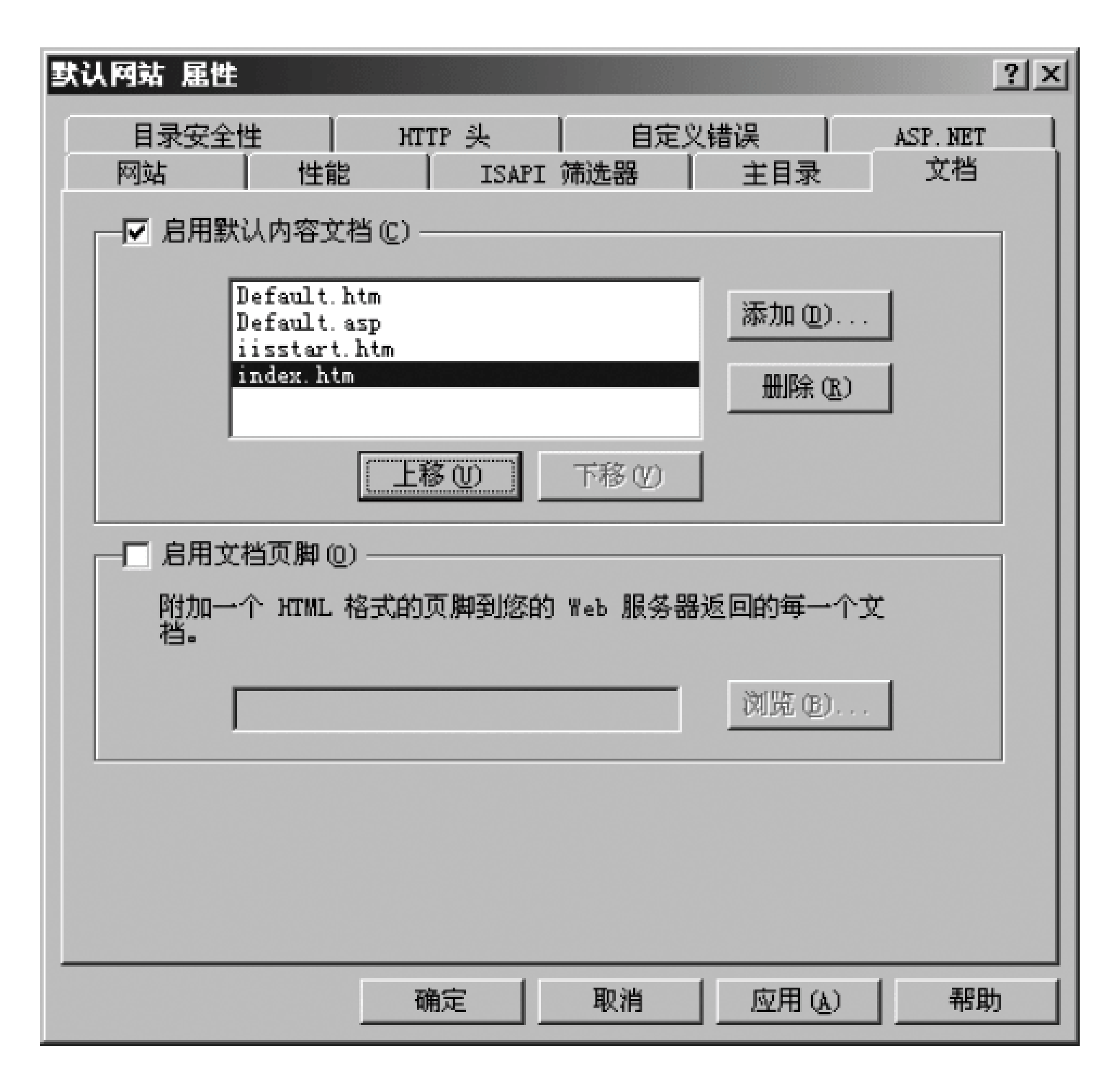


图 9-7　文档设置

单击“添加”按钮，可以添加多个默认文档。若有多个默认文档，系统会先读取最上面的文件，若在站点的主目录内没有该文件，则依次读取后面的文件。为了提高读取速度，建议删除其他不存在的默认文档，同时把真正首页的文件名通过单击“上移”按钮将其移动到最顶部。

9.3　创建 Web 站点和虚拟目录

每个 Web 站点都有一个主目录，对 Web 站点的访问实际上是对站点主目录中内容的访问。如果要通过主目录发布信息，需要将所有网页都保存到网站的主目录中，或将其组织到主目录的子目录中，保证用户可以访问主目录及其子目录中的所有文件。

通过使用虚拟目录，可以将网页文件存储到主目录以外的其他文件夹内，这个文件夹可以位于本地计算机，也可位于别的计算机。虚拟目录是把非主目录内的内容映射到主目录内，每个虚拟目录都有一个别名。

9.3.1　在同一服务器上创建多个 Web 站点

在 Internet 中，每个 Web 站点都具有唯一的标识，这个标识由 IP 地址、端口号和主机头名称这 3 个部分共同决定。根据网站标识的组成，可以通过 3 种方式，在一台计算机上建立多个不同的网站。

(1) 利用不同的主机头名称。此时计算机只需要一个 IP 地址，就可以创建多个网站。利用主机头名称来区分每一个网站。

(2) 利用不同的 TCP 端口。此时每一个网站都使用一个非标准的 Web 服务端口(即非 TCP 80 端口),利用端口号来区分每一个网站。这种方法适合内部 Web 网站、测试网站使用,但不适合于商业网站。

(3) 利用不同的 IP 地址。在一台计算机的网卡上绑定多个 IP,每一个网站分配唯一的 IP 地址,利用 IP 地址来区分每一个网站。

1. 利用不同的主机头名建立不同的网站

按照表 9-1 中的要求,利用同一个 IP 地址、同一个端口,但不同的主机头来建立两个不同的网站 ftp. xyz. net 和 vod. xyz. net。

表 9-1　利用不同的主机头名建立不同的网站

主机头名称	IP 地 址	端 口 号	主 目 录
ftp. xyz. net	192. 168. 10. 1	80	C:\wwwroot1
vod. xyz. net	192. 168. 10. 1	80	C:\wwwroot2

在 C 盘根目录下,新建 wwwroot1 文件夹,作为网站 ftp. xyz. net 的主目录;另外新建 wwwroot2 文件夹,作为网站 vod. xyz. net 的主目录,分别在这两个文件夹内建立内容不同的 index. htm 文件,作为这两个网站的默认首页,以便测试使用。

事先要把与主机头名 ftp. xyz. net 和 vod. xyz. net 相对应的 IP 地址 192. 168. 10. 1 注册到 DNS 服务器内。

完成上述准备工作后,开始创建 ftp. xyz. net 网站,操作步骤如下。

(1) 打开“Internet 信息服务(IIS)管理器”,右击“网站”→选择“新建”→“网站”。

(2) 出现“欢迎使用网站创建向导”对话框时,单击“下一步”按钮。在图 9-8 中,输入此网站的描述,单击“下一步”按钮。

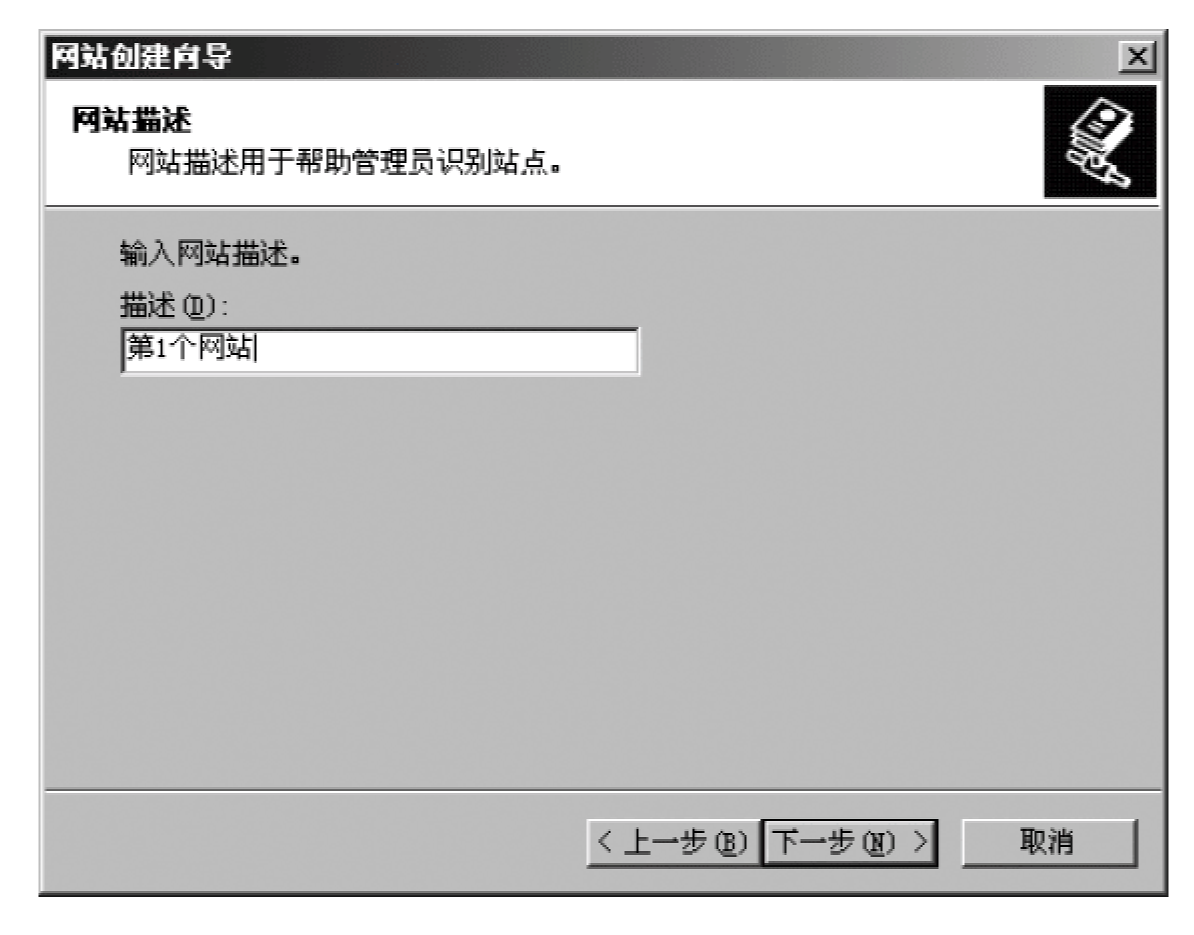


图 9-8　指定网站描述

(3) 在图 9-9 中,在“此网站的主机头”后的文本框中输入 ftp. xyz. net,单击“下一步”

按钮。

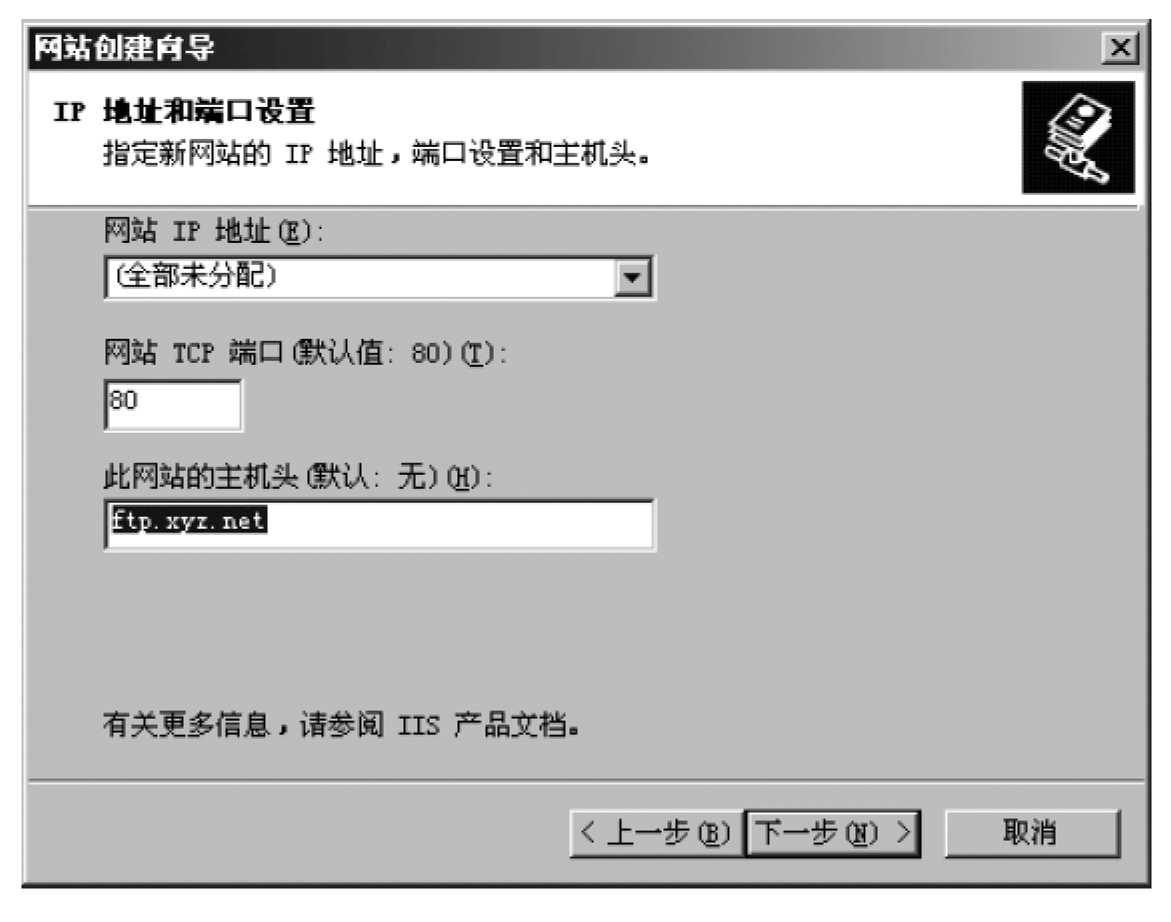


图 9-9　指定网站 IP 地址、端口和主机头

(4) 在图 9-10 中，选择网站 ftp. xyz. net 的主目录所对应的路径，在“路径”中输入路径 C:\wwwroot1，也可以单击“浏览”按钮选择路径，单击“下一步”按钮。

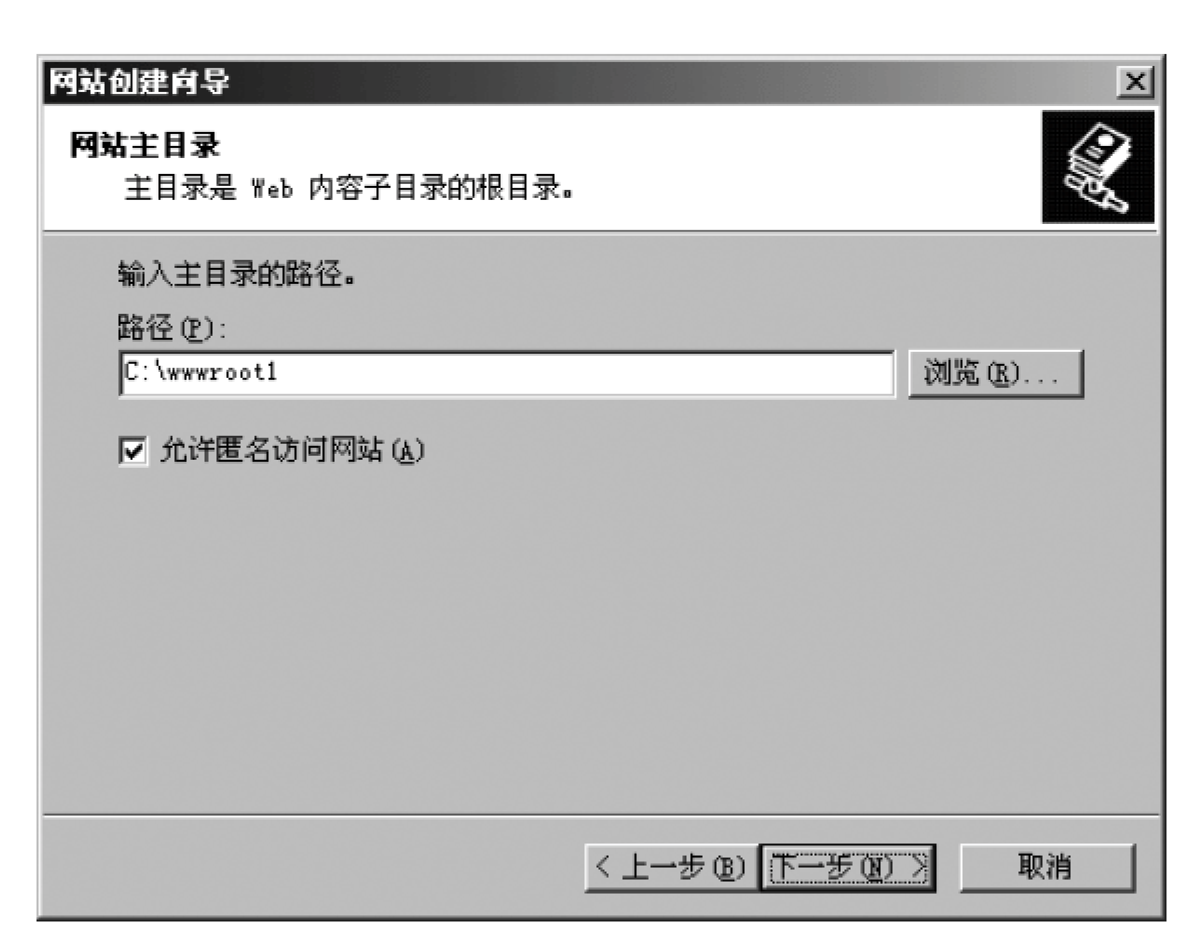


图 9-10　指定网站主目录

(5) 在图 9-11 中，设置好权限后单击“下一步”按钮。

(6) 出现“您已经成功完成网站创建向导”对话框时，单击“完成”按钮即可完成 ftp. xyz. net 网站的创建。

利用类似的方法，创建主机头为 vod. xyz. net 的网站。

打开客户端计算机的浏览器，在地址栏内输入 http://vod. xyz. net、http://ftp. xyz. net，就可以连接网站，并测试所创建的网站是否能正常运行。

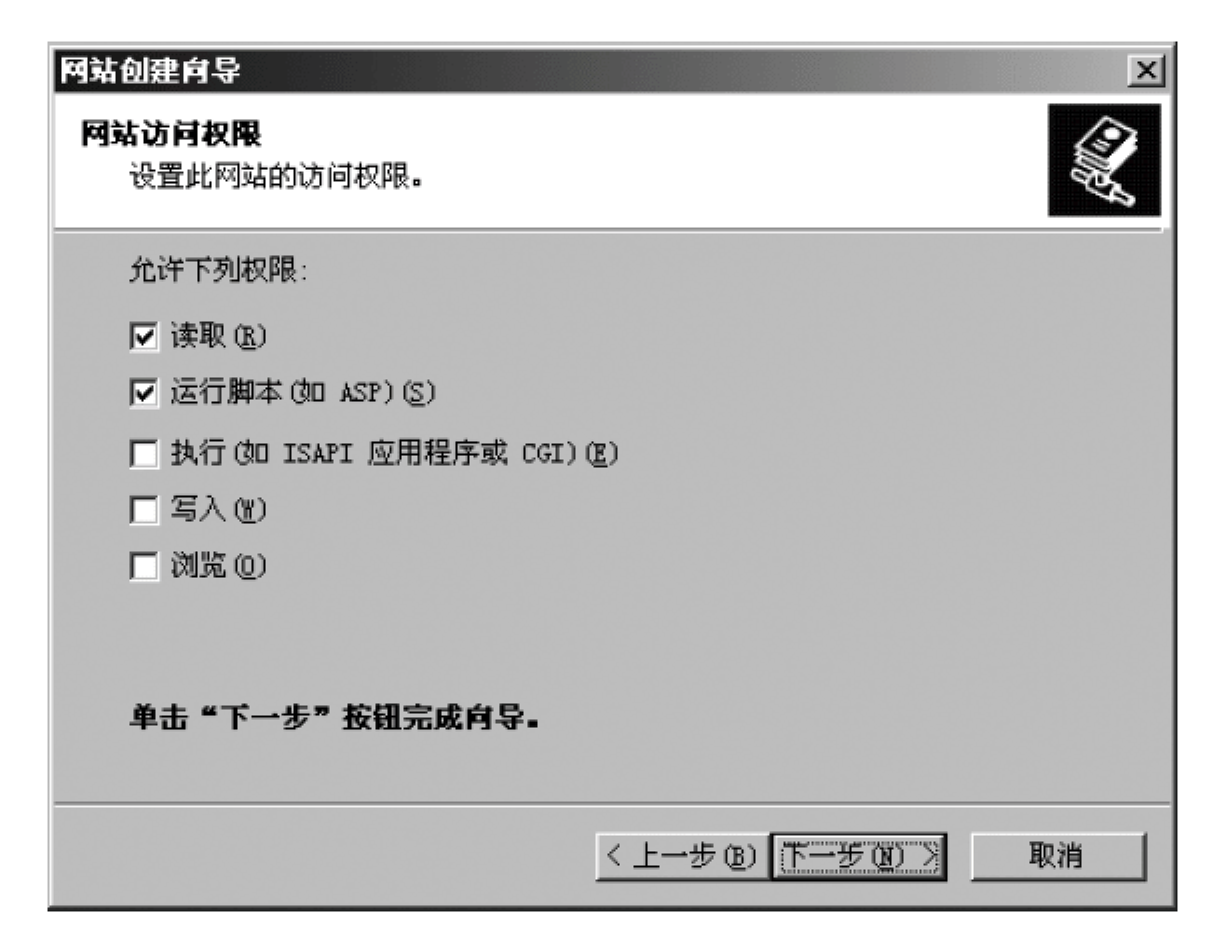


图 9-11 指定网站访问权限

2. 利用 TCP 连接端口建立多个网站

按照表 9-2 中的要求,利用同一个 IP 地址、同一个主机头、不同的端口来建立两个不同的网站 server1. xyz. net:8080 和 server1. xyz. net:8081。

表 9-2 利用 TCP 连接端口建立多个网站

主机头名称	IP 地 址	TCP 端口号	主 目 录
server1. xyz. com	192. 168. 10. 2	8080	C:\wwwroot3
server1. xyz. com	192. 168. 10. 2	8081	C:\wwwroot4

在 C 盘根目录下,新建 wwwroot3 文件夹,作为网站 server1. xyz. net:8080 的主目录;另外新建 wwwroot4 文件夹,作为网站 server1. xyz. net:8081 的主目录,然后分别在这两个文件夹内建立内容不同的 index. htm 文件,作为网站的默认网页,以便测试使用。

事先要把与主机头名 server1. xyz. net 相对应的 IP 地址 192. 168. 10. 2 注册到 DNS 服务器内。

完成上述准备工作后,开始创建 server1. xyz. net:8080 网站,操作步骤如下。

(1) 打开“Internet 信息服务(IIS)管理器”,右击“网站”→选择“新建”→“网站”。

(2) 出现“欢迎使用网站创建向导”对话框时,单击“下一步”按钮。在图 9-12 中,输入此网站的描述后,单击“下一步”按钮。

(3) 在图 9-13 中,指定网站 TCP 端口,在此输入 8080,单击“下一步”按钮。

(4) 在图 9-14 中,输入网站 server. xyz. net 的主目录的路径,可以在“路径”中输入路径 C:\wwwroot3,也可以单击“浏览”按钮指定路径,单击“下一步”按钮。

(5) 出现图 9-15 时,保持默认的权限不变,单击“下一步”按钮。

(6) 出现“您已经成功完成了网站创建向导”对话框时,单击“完成”按钮即可完成 server1. xyz. net:8080 网站的创建。

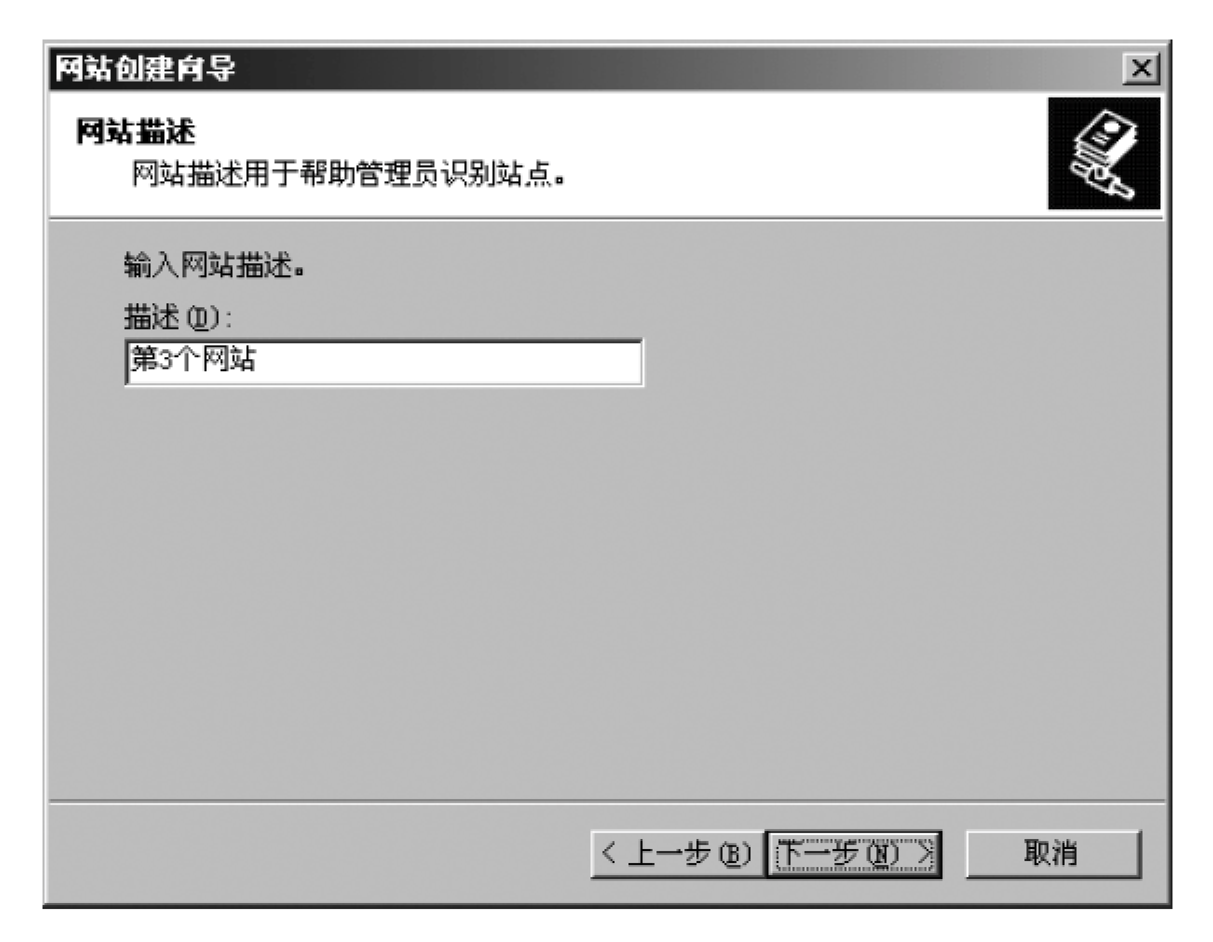


图 9-12　指定网站描述

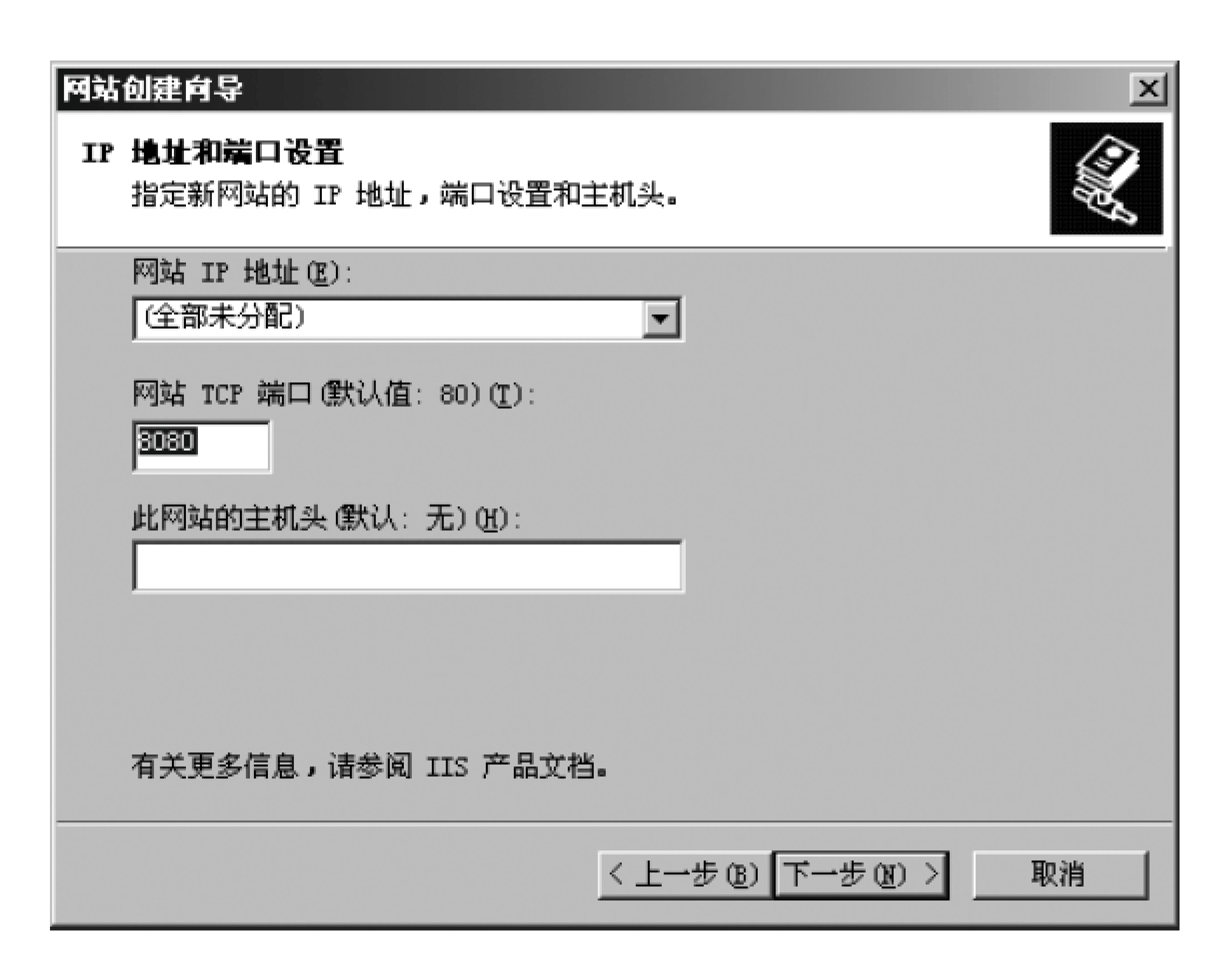


图 9-13　指定网站 TCP 端口

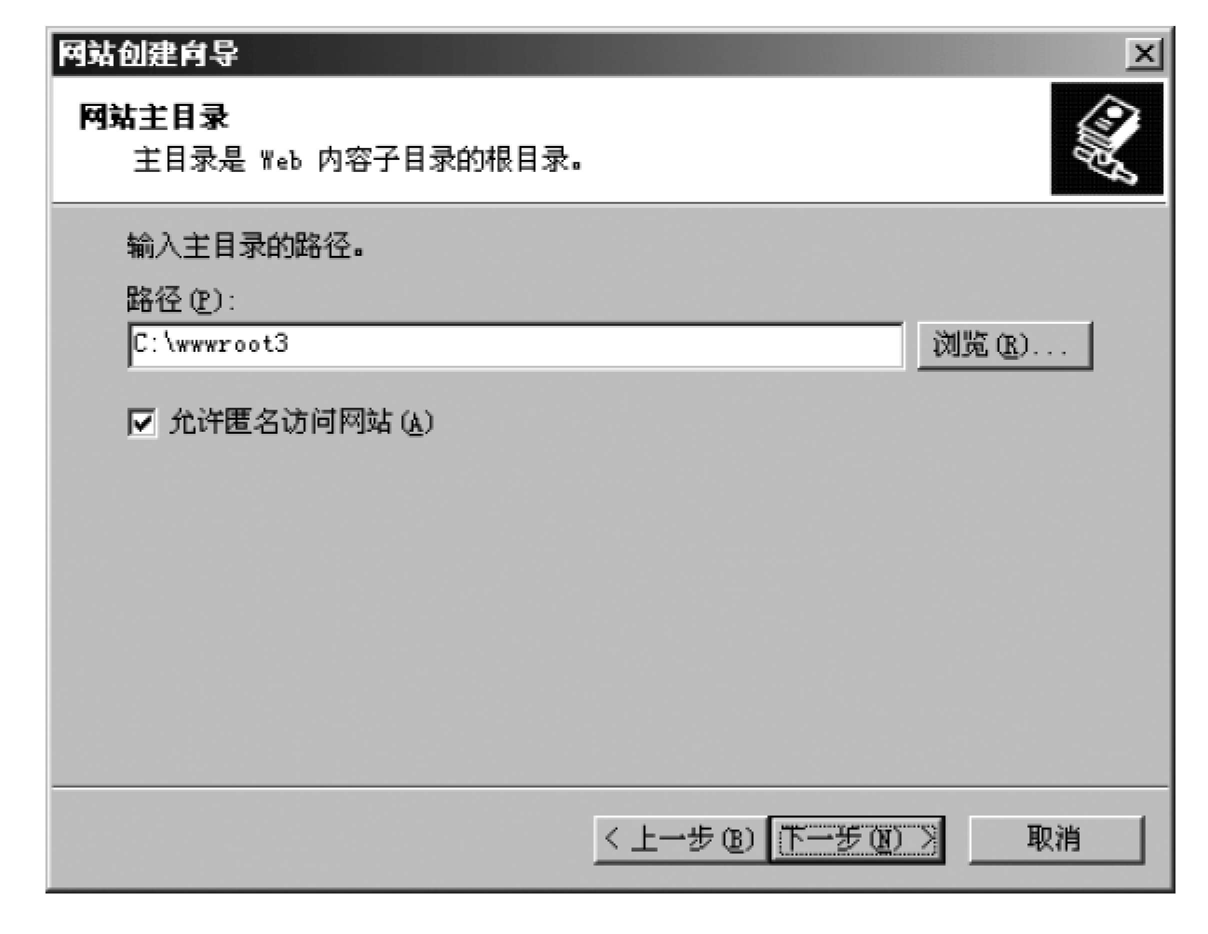


图 9-14　指定网站主目录

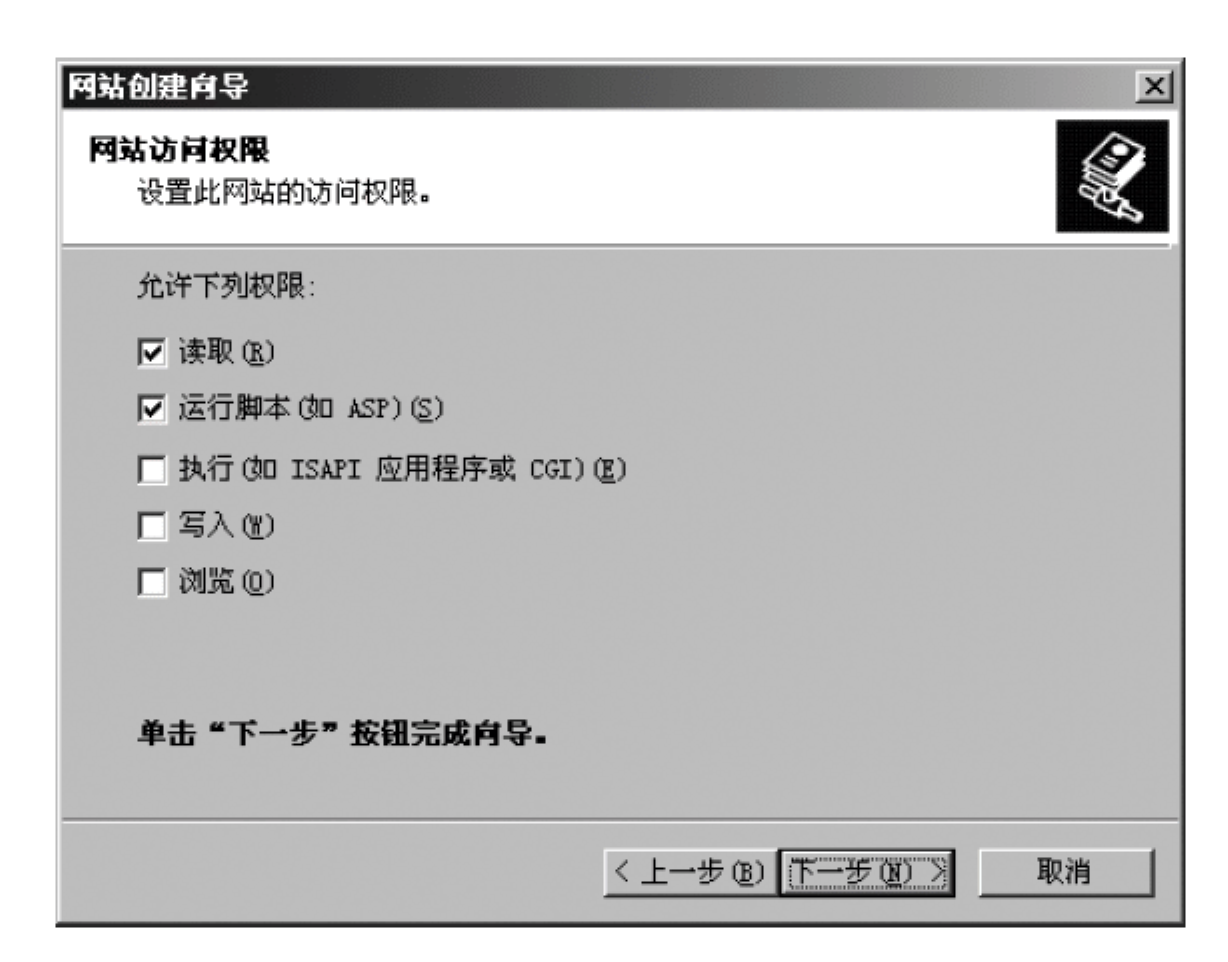


图 9-15　指定网站的访问权限

利用类似的方法,创建立名为 server. xyz. net:8081 的网站。

打开客户端计算机的浏览器,在地址栏内输入 http://server1. xytz. net:8080、http://server1. xytz. net:8081,就可以连接网站,并测试所创建的网站是否能正常运行。

3. 利用多个 IP 地址建立多个网站

在一个网卡上可以绑定多个 IP 地址,利用绑定的多个 IP 地址就可以在同一台 Web 服务器上建立多个不同的网站。按照表 9-3 中的要求,利用同一个端口,但不同的 IP 地址,在同一台 Web 服务器上建立两个不同的网站 server2. xyz. net 和 server3. xyz. net。

表 9-3　利用多个 IP 地址建立多个网站

主机头名称	IP 地址	端口号	主目录
server2. xyz. net	192. 168. 10. 3	80	C:\wwwroot5
server3. xyz. net	192. 168. 10. 4	80	C:\wwwroot6

在 C 盘根目录下,新建 wwwroot5 文件夹,作为网站 server2. xyz. net 的主目录;另外新建 wwwroot6 文件夹,作为网站 server3. xyz. net 的主目录,然后分别在这两个文件夹内建立内容不同的 index. htm 文件,作为网站的默认网页,以便测试使用。

首先要在 Web 服务器上绑定多个 IP 地址,操作步骤为:右击"网上邻居"→"属性"→"本地连接"→"属性"→"Internet 协议(TCP/IP)"→"属性"→"高级",单击"IP 地址"下的"添加"按钮,添加 IP 地址 192. 168. 10. 3 和 192. 168. 10. 4,完成后如图 9-16 所示。

还要把与主机头名 server2. xyz. net 和 server3. xyz. net 相对应的 IP 地址 192. 168. 10. 3 和 192. 168. 10. 4 注册到 DNS 服务器。

完成上述准备工作后,开始创建 server2. xyz. net 网站,操作步骤如下。

(1) 打开"Internet 信息服务(IIS)管理器",右击"网站"→选择"新建"→"网站"。

(2) 出现"欢迎使用网站创建向导"对话框时,单击"下一步"按钮。在图 9-17 中,输

入此网站的描述，单击“下一步”按钮。

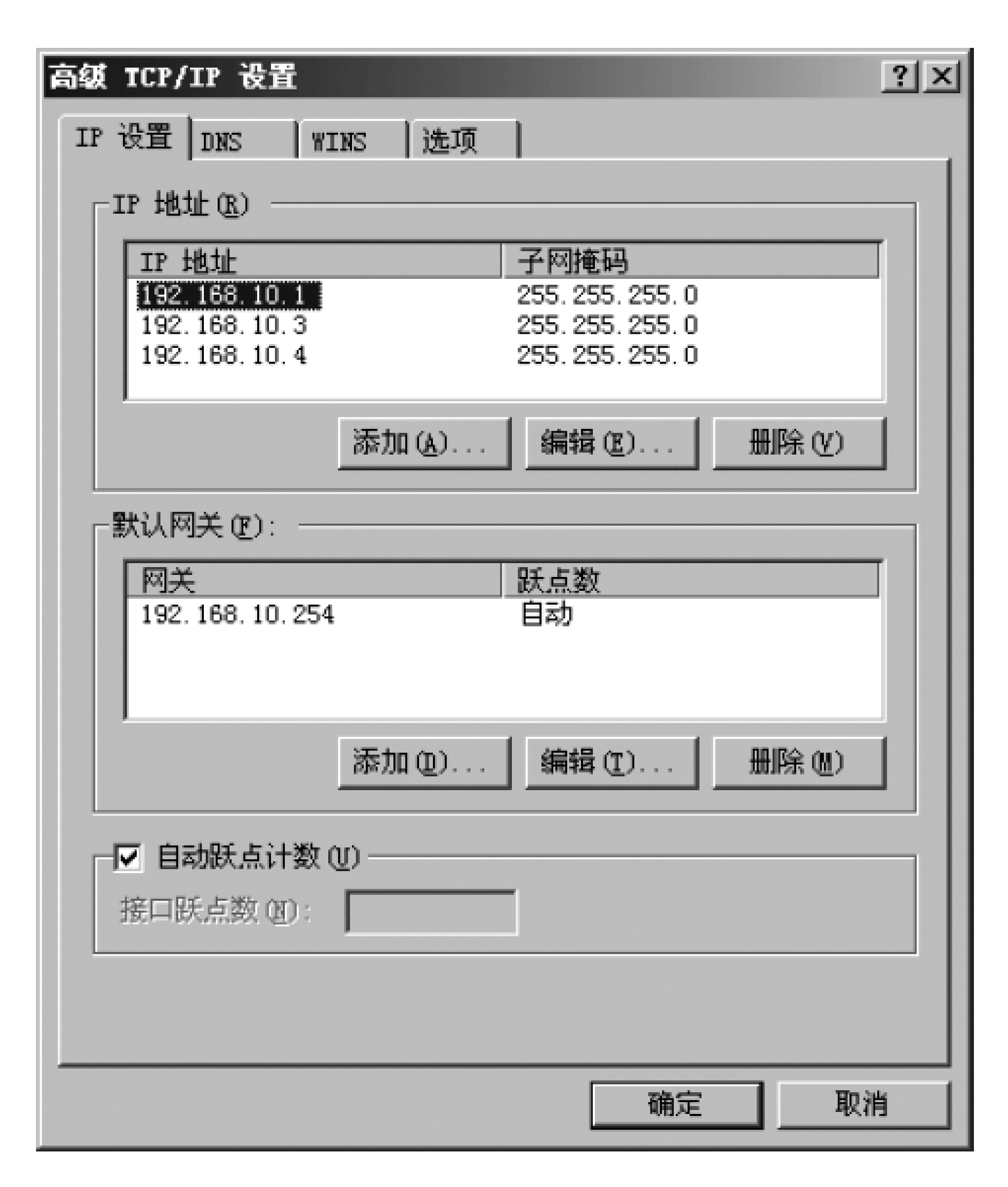


图 9-16 绑定多个 IP 地址

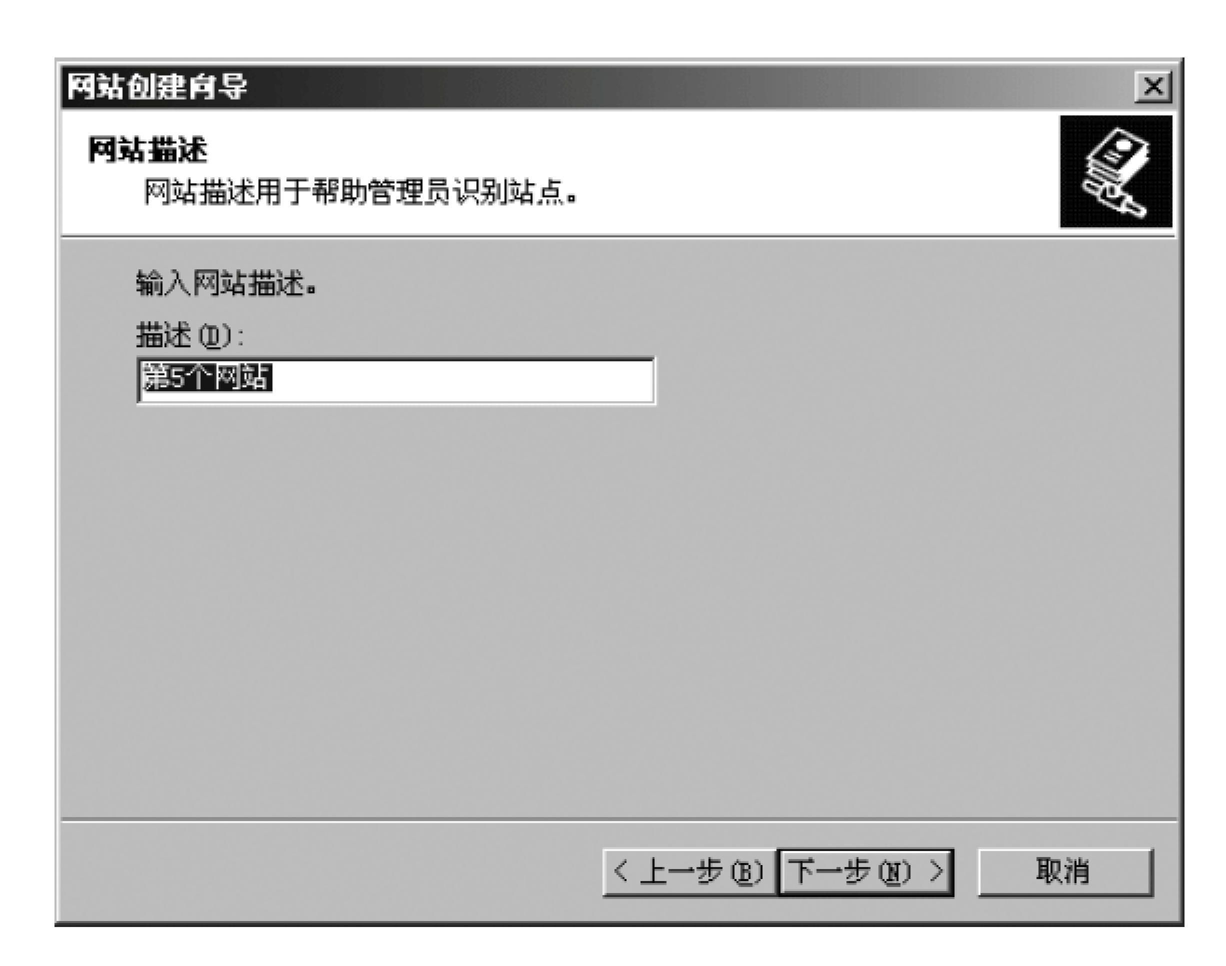


图 9-17 指定网站描述

(3) 在图 9-18 中，在“网站 IP 地址”下拉列表中，选择需要绑定的 IP 地址，单击“下一步”按钮。

(4) 在图 9-19 中，选择网站 server2.xyz.net 的主目录所对应的路径，可以在“路径”中输入路径 C:\wwwroot5，也可以单击“浏览”按钮来指定路径，单击“下一步”按钮。

(5) 出现图 9-20 时，单击“下一步”按钮。

(6) 出现“您已经成功完成了网站创建向导”对话框时，单击“完成”按钮即可创建 IP 地址为 192.168.10.3 的网站。

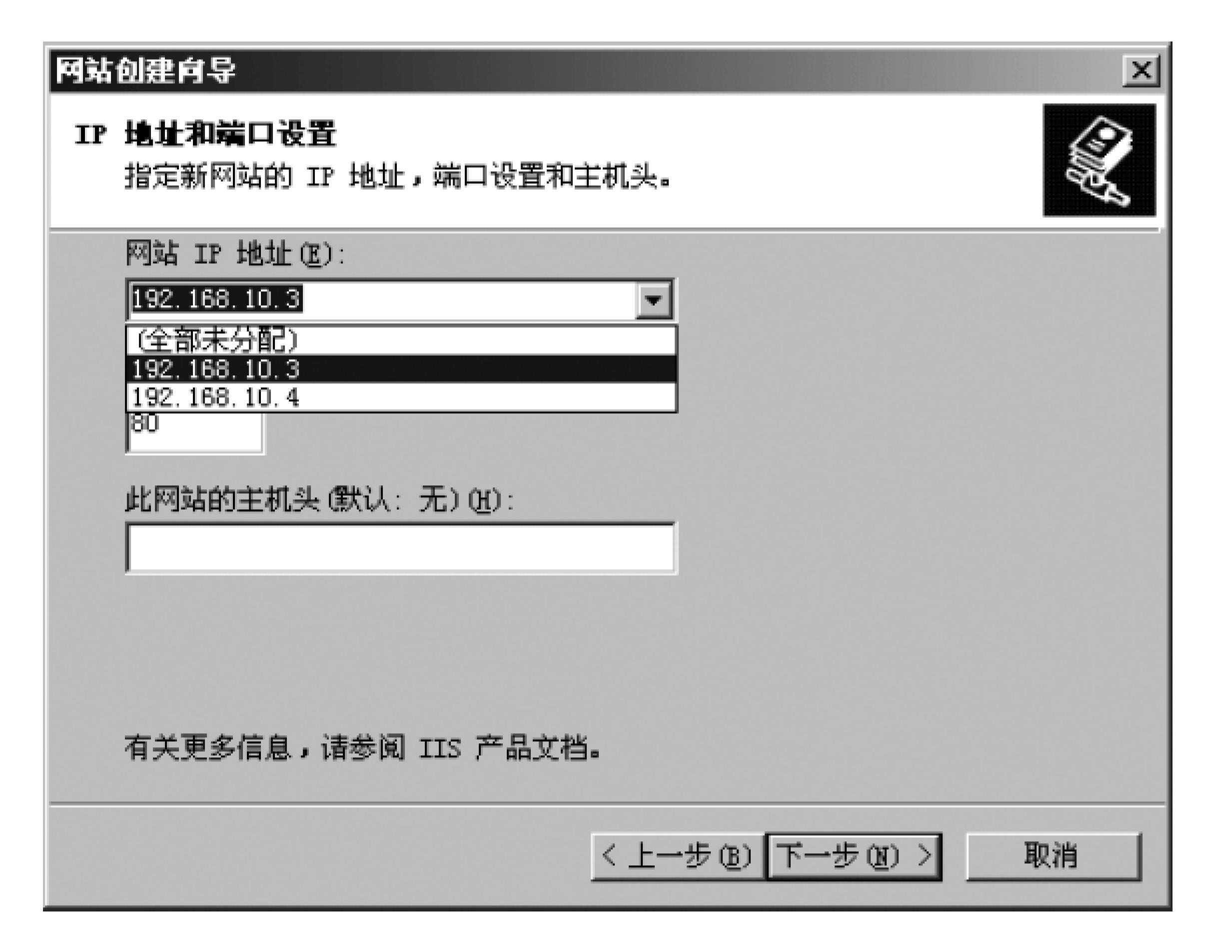


图 9-18　指定网站的 IP 地址

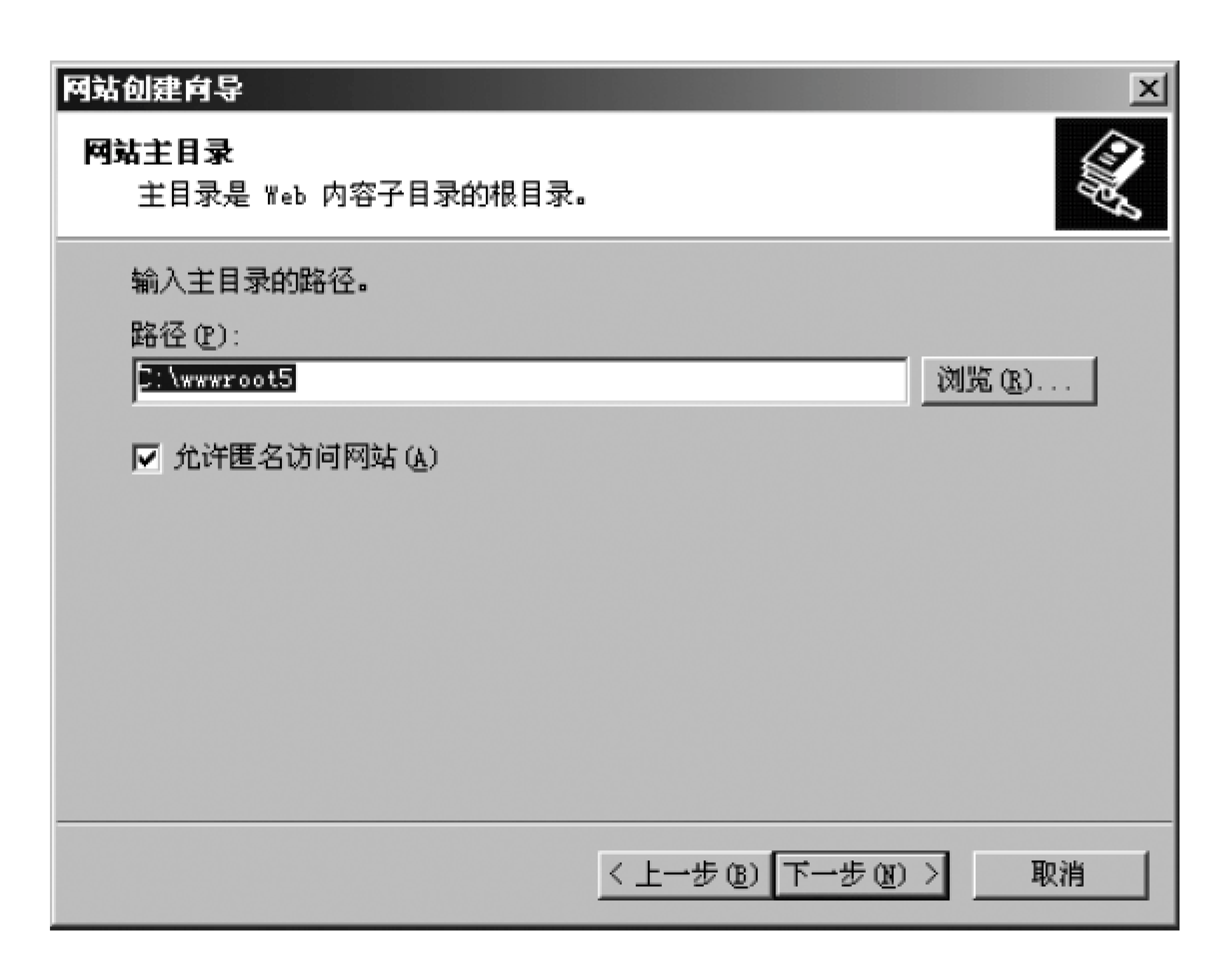


图 9-19　指定网站的主目录

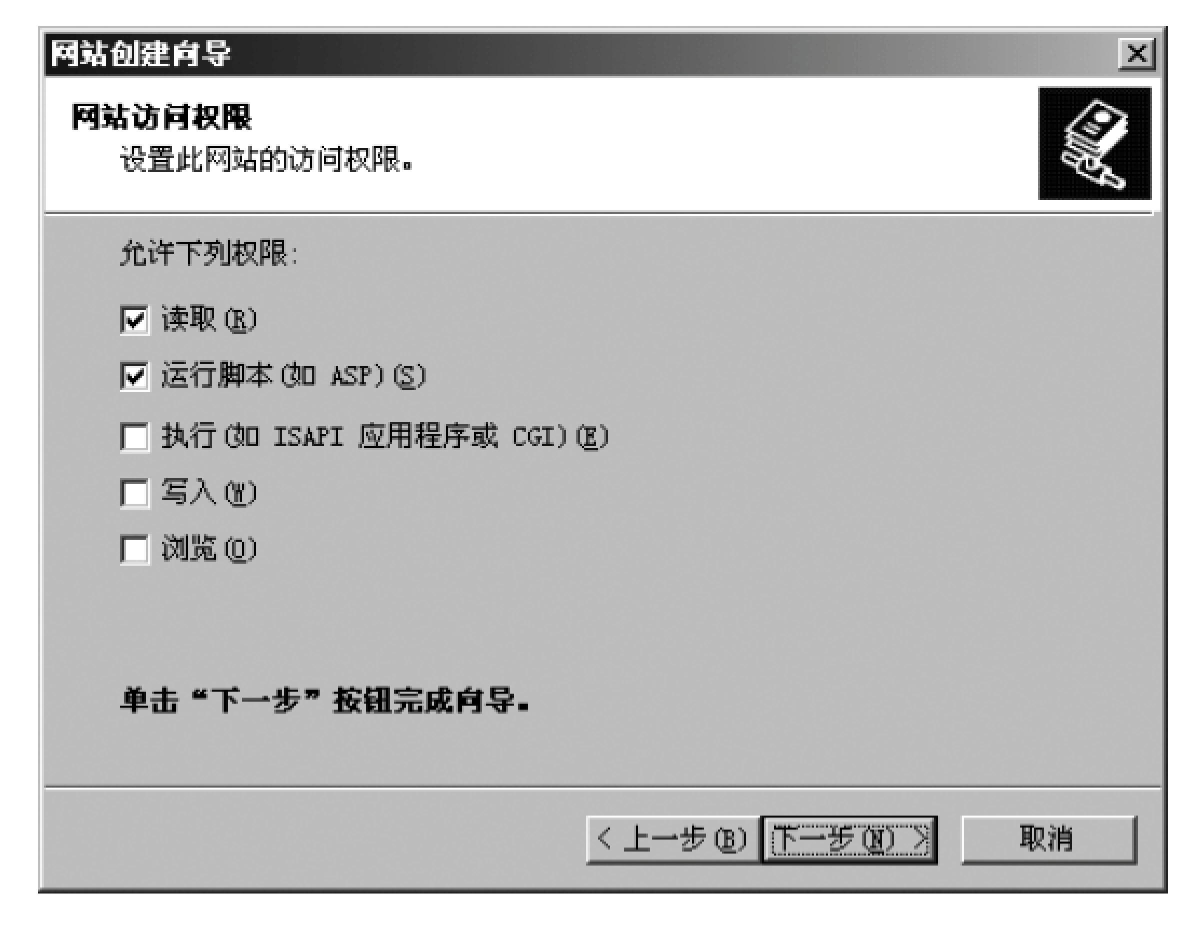


图 9-20　设置网站的访问权限

利用类似的方法创建IP地址为192.168.10.4的网站。

打开客户端计算机的浏览器，在地址栏内输入 http://server2.xyz.net、http://server3.xyz.net，就可以连接网站，并测试所创建的网站是否能正常运行。

9.3.2 创建虚拟目录

虚拟目录是Web站点发布信息的重要方式。虚拟目录可以把站点主目录之外的内容映射到主目录内，就像是主目录中的内容一样。而这些内容可以是本地计算机上的目录，或者是另一台计算机上的共享目录或是一个URL。物理目录的存放路径对虚拟目录别名没有任何影响。

利用虚拟目录发布网站，客户端在浏览器中输入“http://IP(域名)/虚拟目录别名”来浏览虚拟目录内的内容。

在主机头名为www.xyz.net的网站内建立虚拟目录，其创建要求如表9-4所示。

表9-4 利用虚拟目录创建网站

主机头名称	IP地址	端口号	目录
www.xyz.net	192.168.10.1	80	C:\Inetpub\wwwroot (默认主目录)
虚拟目录别名 vod	192.168.10.1	80	D:\vodceshi(虚拟目录的物理路径)

在D盘新建vodceshi文件夹，作为网站www.xyz.net的虚拟目录对应的物理目录，并在此文件夹内建立和主目录的首页内容不同的index.htm文件，以便测试使用。

为了让用户能够正常浏览利用虚拟目录发布的网站 http://www.xyz.net/vod，需要把与主机头名www.xyz.net相对应的IP地址192.168.10.1注册到DNS服务器，并配置好主目录为C:\Inetpub\wwwroot的默认网站。

做好上述准备工作后，开始在默认网站内建立虚拟目录，操作步骤为如下。

(1) 打开“Internet信息服务(IIS)管理器”，选择“网站”，右击“默认网站”，选择“新建”→“虚拟目录”。

(2) 出现“欢迎使用虚拟目录创建向导”对话框时，单击“下一步”按钮。在图9-21中，为虚拟目录设置一个别名，单击“下一步”按钮。

(3) 在图9-22中，选择虚拟目录所对应的物理目录的路径，可以在“路径”中输入路径D:\vodceshi，或者单击“浏览”按钮指定路径，单击“下一步”按钮。

(4) 出现图9-23时，单击“下一步”按钮。

(5) 出现“您已顺利完成虚拟目录创建向导”对话框时，单击“完成”按钮即可完成别名为vod、物理目录路径为D:\vodceshi的虚拟目录的创建。如图9-24所示，虚拟目录的图标为齿轮形状。

打开客户端计算机的浏览器，在地址栏内输入 http://www.xyz.net/vod/，来连接网站以测试所建立的虚拟目录内的内容是否能正常运行。

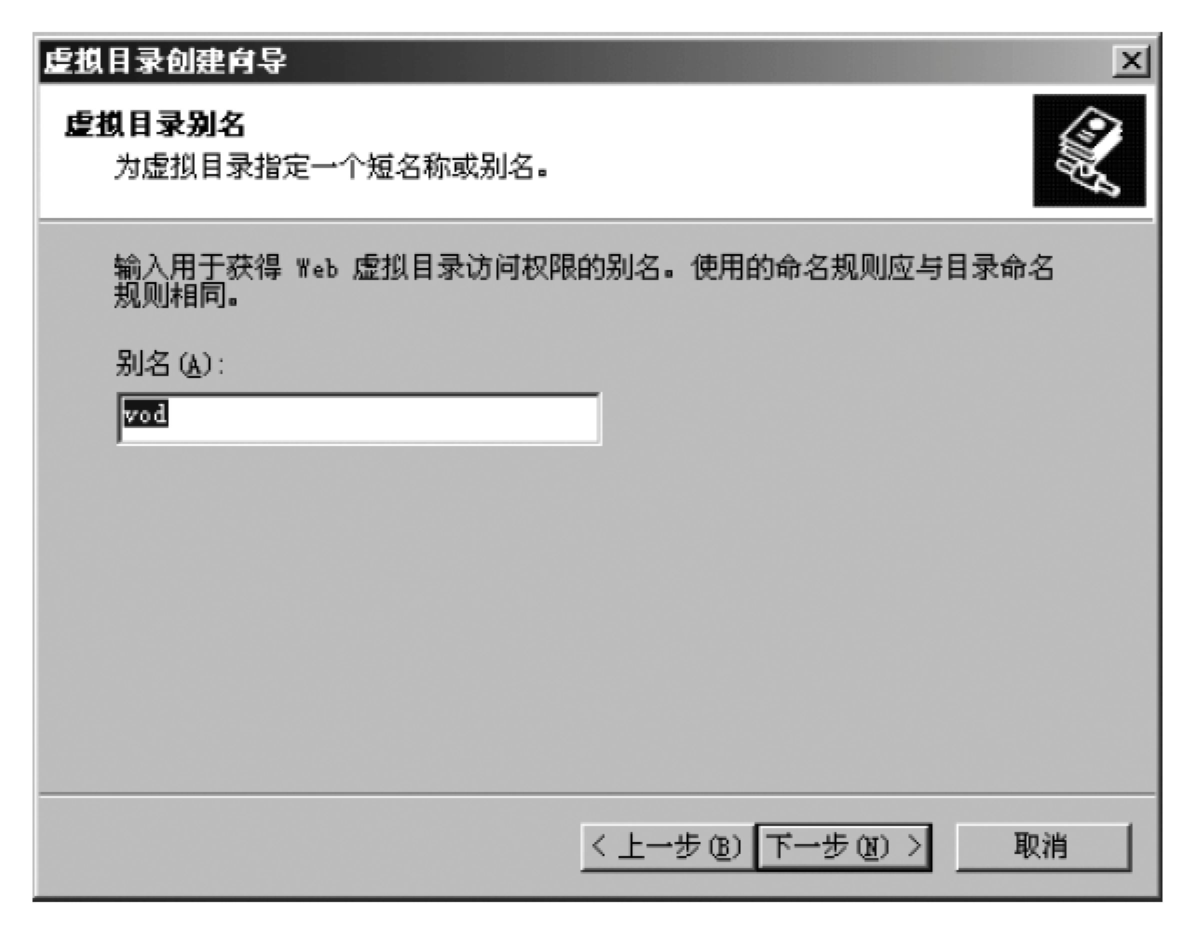


图 9-21　为虚拟目录设置一个别名

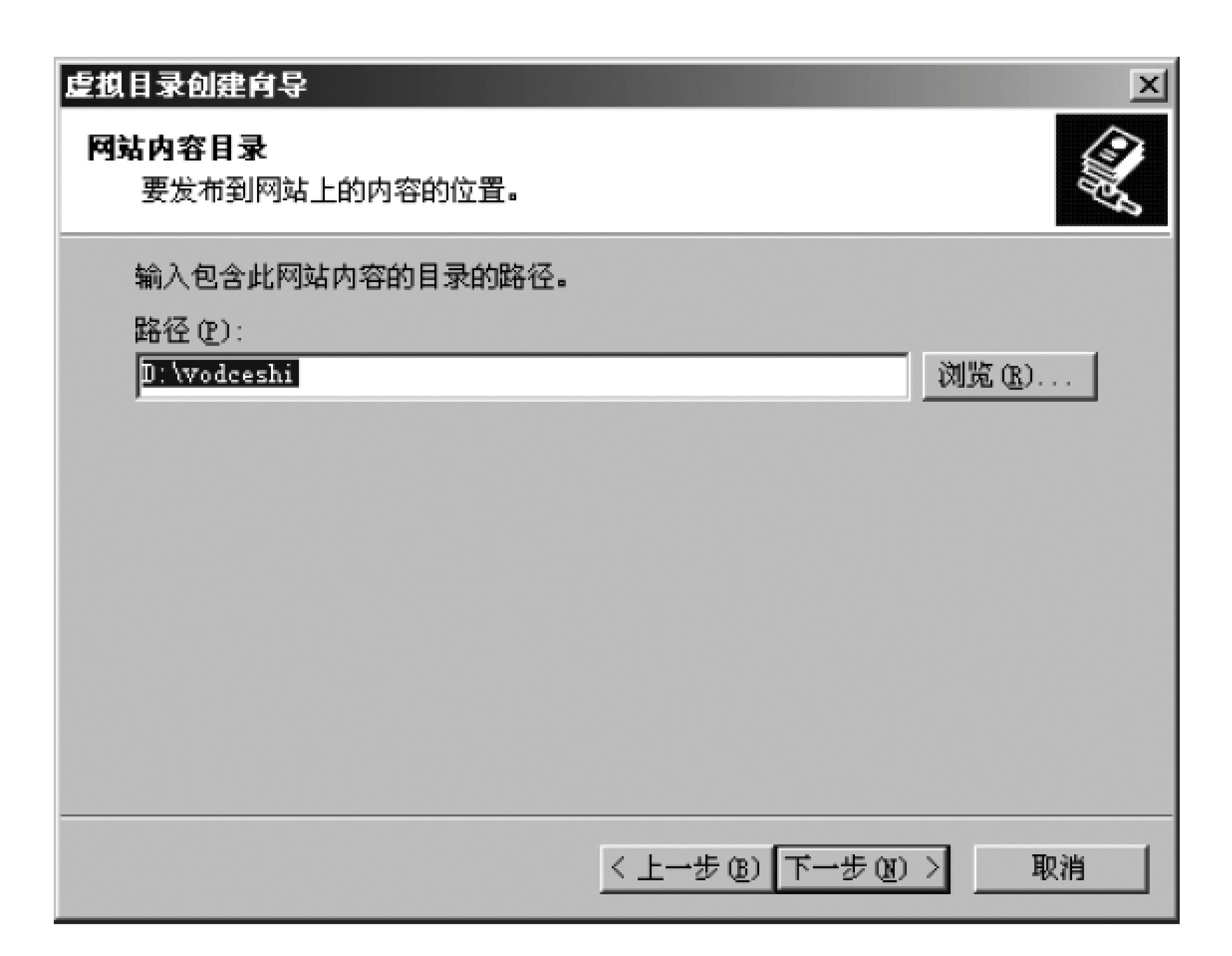


图 9-22　选择虚拟目录所对应的物理目录的路径

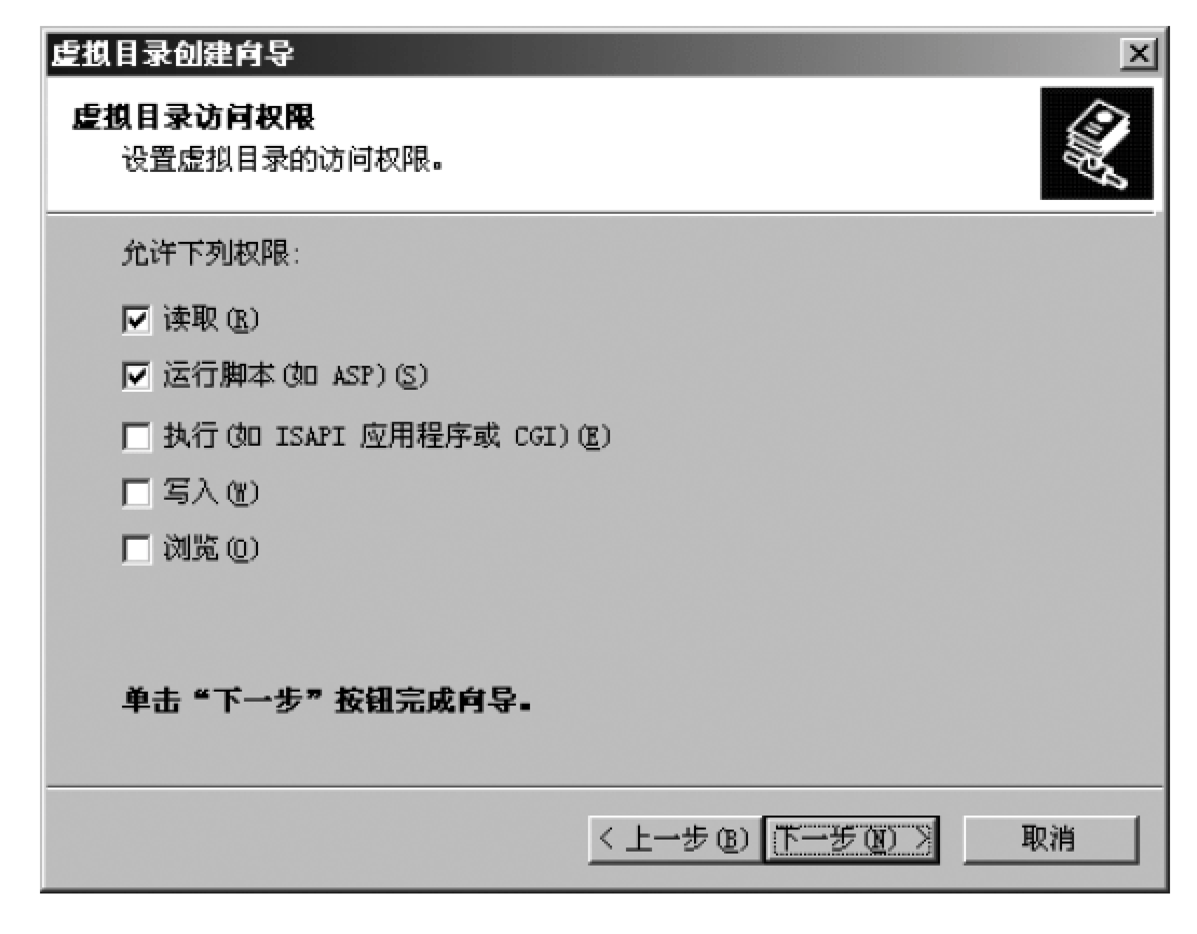


图 9-23　设置虚拟目录的访问权限



图 9-24　创建的虚拟目录

9.4　网站安全性设置

默认情况下，Windows Server 2003 中安装的 IIS 只支持静态网页，其他相应的服务处于“停止”状态，以减少入侵者攻击的机会。管理员可以根据需要自行安装相关组件、启用相关服务。通过访问认证方式和访问权限的设置，在一定程度上能保证 Web 服务器的安全性。

9.4.1　用户身份验证方法

用户身份验证是指用户在访问服务器上的资源时，需要提供有效的用户名和密码，只有通过验证之后，用户才可以访问资源。IIS 提供的安全验证方法有匿名验证、基本身份验证、摘要式验证和集成 Windows 身份验证。

以默认网站为例，要设置网站验证方法，操作步骤为：打开“Internet 信息服务(IIS)管理器”，选择网站，右击“默认网站”，选择“属性”，打开如图 9-25 所示的“目录安全性”选项卡。

单击“身份验证和访问控制”区域中的“编辑”按钮，出现图 9-26。

1. 启用匿名访问

启用匿名访问允许所有客户访问网站的公开信息，不需要提供用户名与密码。所有的浏览器都支持匿名验证。当用户尝试连接 Web 站点时，服务器会利用在安装 IIS 时自动建立的“IUSR_计算机名称”用户账户作为匿名账户。

也可以自行选择匿名账户，先在 Active Directory 数据库或本机安全账户数据库内建立此账户，然后在图 9-26 中单击“浏览”按钮选择此账户并输入账户的密码。如果网站启用了匿名验证，同时又选取其他的验证方法，则 IIS 会先利用匿名方法来验证用户的身份。

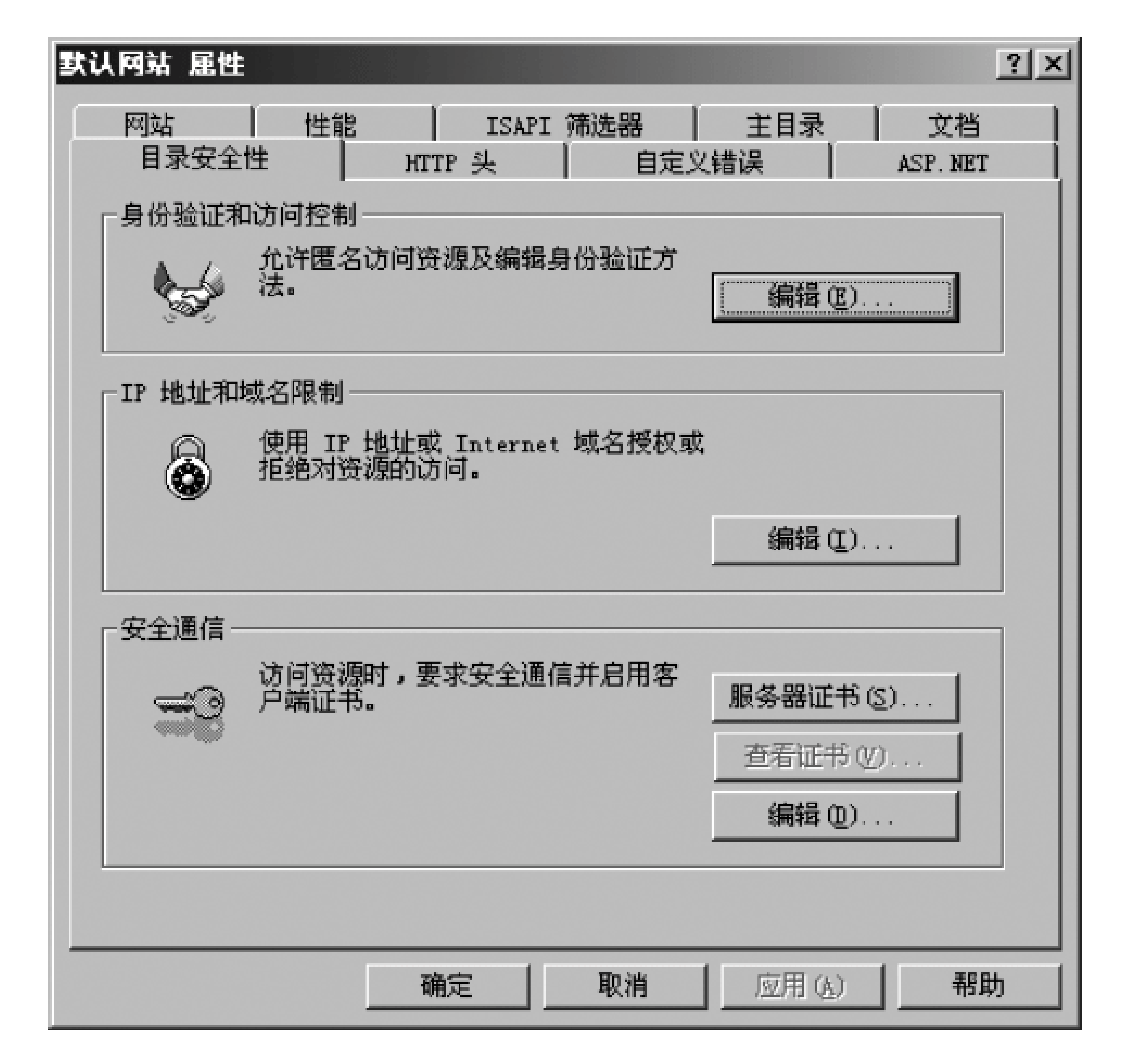


图 9-25 “目录安全性”选项卡

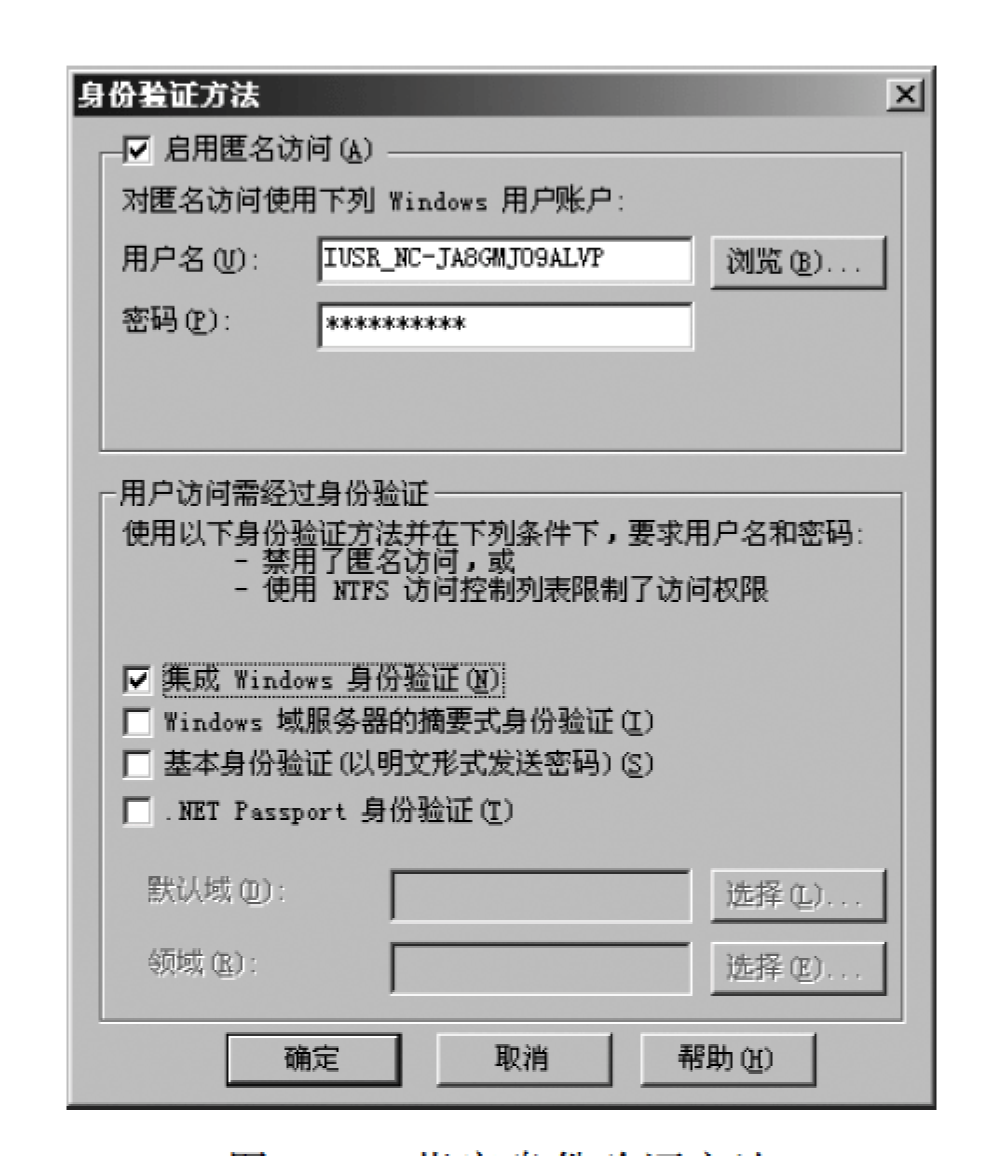


图 9-26 指定身份验证方法

2. 集成 Windows 身份验证

集成 Windows 身份验证要求用户输入用户名与密码，集成 Windows 身份验证支持两种验证方法，分别为 Kerberos V5 和 NTLM 验证。集成 Windows 身份验证是 Windows Server 2003 默认使用的验证方法。

在客户端计算机上，用户可以设置是要自动利用登录的账户来连接网站，还是要求用户自行输入用户名与密码，其设置方法：打开 IE 的“工具”菜单→“Internet 选项”，选择网

站所在区域,选择“安全”选项卡,如图9-27所示。

单击“自定义级别”按钮,出现图9-28,在“用户验证”下的“登录”内,选择合适的登录验证方式。



图9-27 设置IE的安全选项

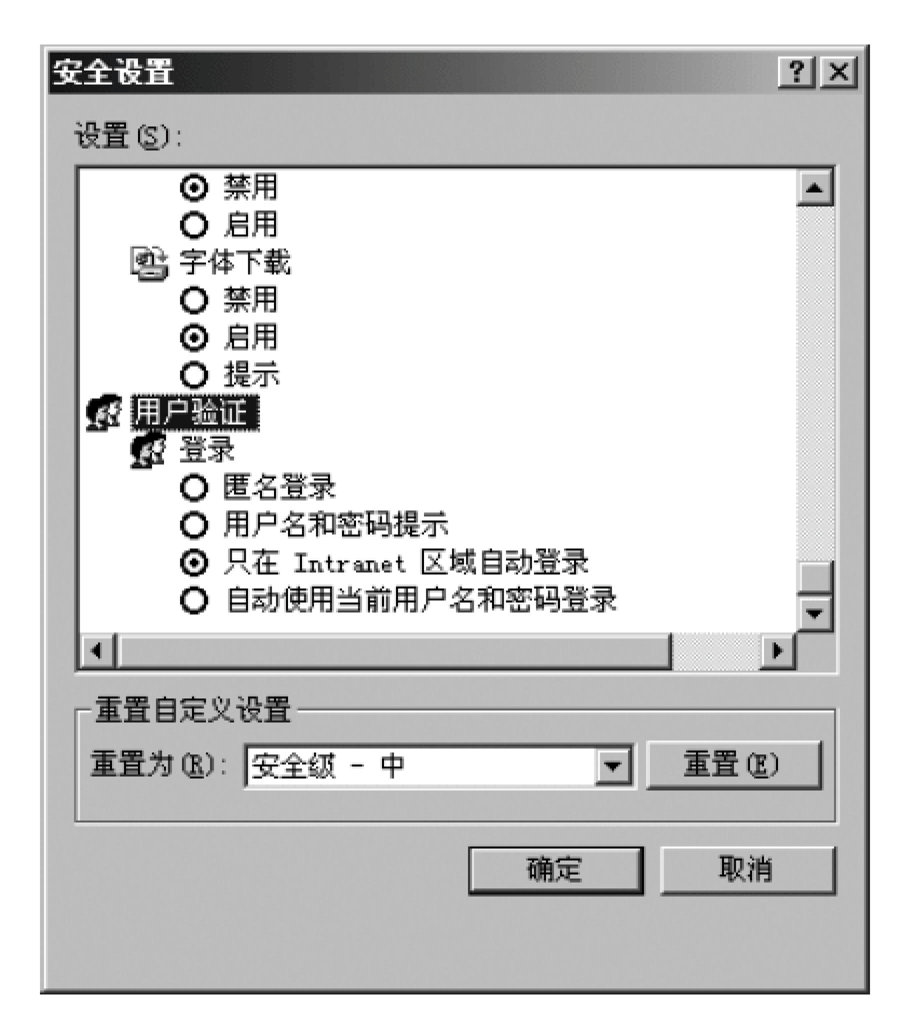


图9-28 设置用户验证的方式

3. Windows域服务器的摘要式身份验证

只有当Web服务器运行在Active Directory域的成员服务器或域控制器上时,才可以启用“Windows域服务器的摘要式身份验证”。用户登录的账户必须是Active Directory内的域用户账户,而且此账户必须Web服务器在同一个域内或是在同一个信任域内。

“Windows域服务器的摘要式身份验证”比“基本身份验证”更安全,因为用户名与密码会经过MD5算法的处理,然后将处理后所产生的散列随机数传送到网站。即使散列随机数被别人截取,别人也没有办法从散列随机数得知用户名与密码。

4. 基本身份验证

基本身份验证是HTTP规范中的一部分,绝大多数的浏览器都支持这种验证方法,该验证过程中,用户名和密码是以明文形式发送的,没有经过加密,因此存在安全问题。

若这是唯一可选的身份验证方法,也应和SSL配合使用,要使用SSL必须获得一个服务器证书,请求用一个特定的端口进行数据传输,同时禁用其他任何形式的身份验证方法。

默认IIS会先利用匿名方式验证用户的身份,为了更好地测试基本身份验证,先将匿名验证的方法停用,选择“基本身份验证(以明文形式发送密码)”。启动基本身份验证,出现图9-29时,单击“是”按钮。

在图 9-30 所示的“默认域”和“领域”内输入以下信息。

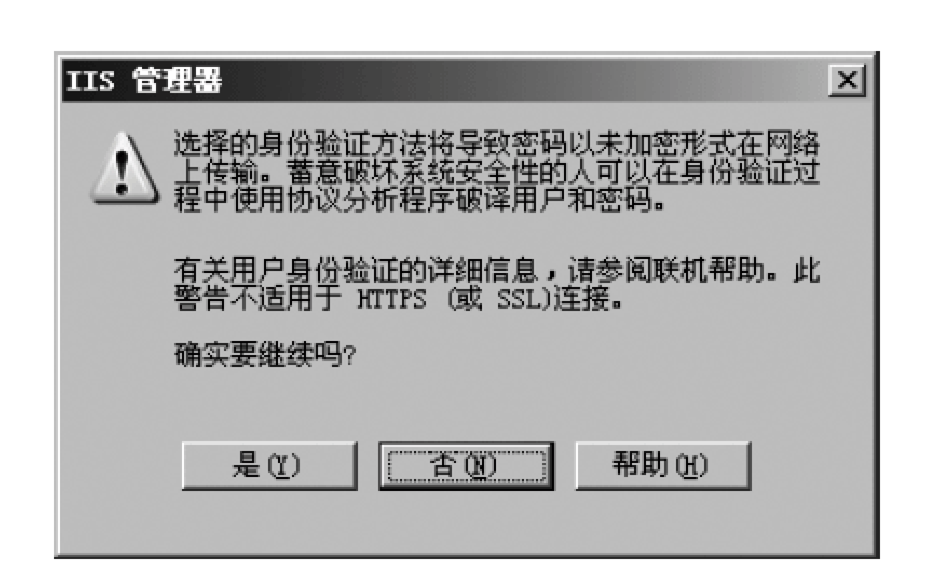


图 9-29　启动基本身份验证时的警告对话框

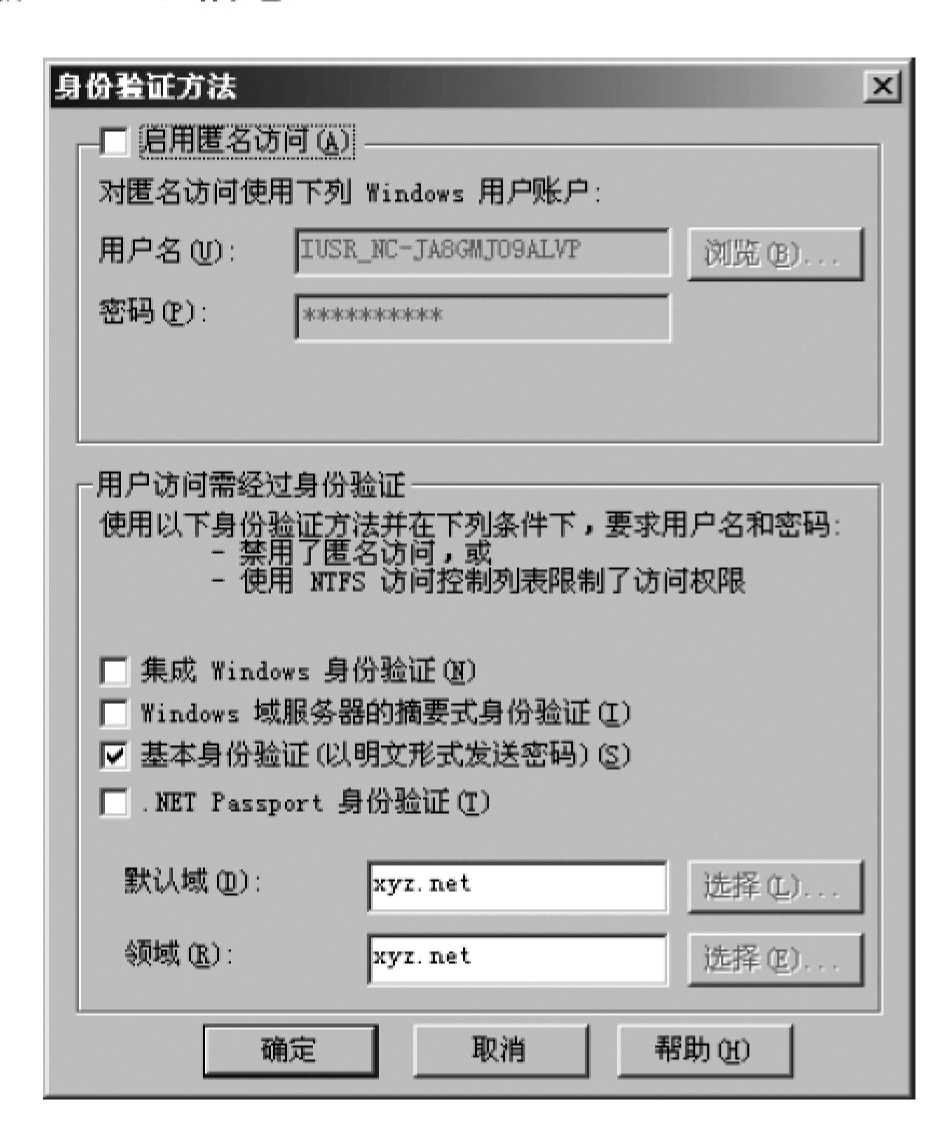


图 9-30　指定默认域和领域信息

(1) 默认域。用来设置用户账户所隶属的域。“默认域”处没有输入信息，如果 IIS 计算机是独立服务器，则以本地安全性数据库来检查用户名称与密码是否正确；如果 IIS 计算机是域控制器，则以 Active Directory 数据库来检查用户名与密码是否正确。

(2) 领域。会被显示在用户登录界面上。

当用户利用浏览器连接启动了基本身份验证的站点时，将显示如图 9-31 所示的界面。



图 9-31　连接到站点时的登录界面

5. .NET Passport 身份验证

此选项是 Windows Server 2003 新增加的内容，它允许在 Web 站点上运行. NET Passport 身份验证服务，使 Web 站点依靠. NET Passport 验证中心来对用户进行身份验证，而不是使用服务器上的身份验证系统。这样用户只需要一个. NET Passport 的用户名和密码就可以访问所有支持. NET Passport 的 Web 站点。

9.4.2　基于 IIS 的权限

在 Web 站点上，右击“属性”，选择“主目录”选项卡，其包含了 Web 站点访问权限和应用程序设置，如图 9-32 所示。

Web 站点的访问权限主要包括 6 种，其中，默认启用读取、记录访问、索引资源 3 种

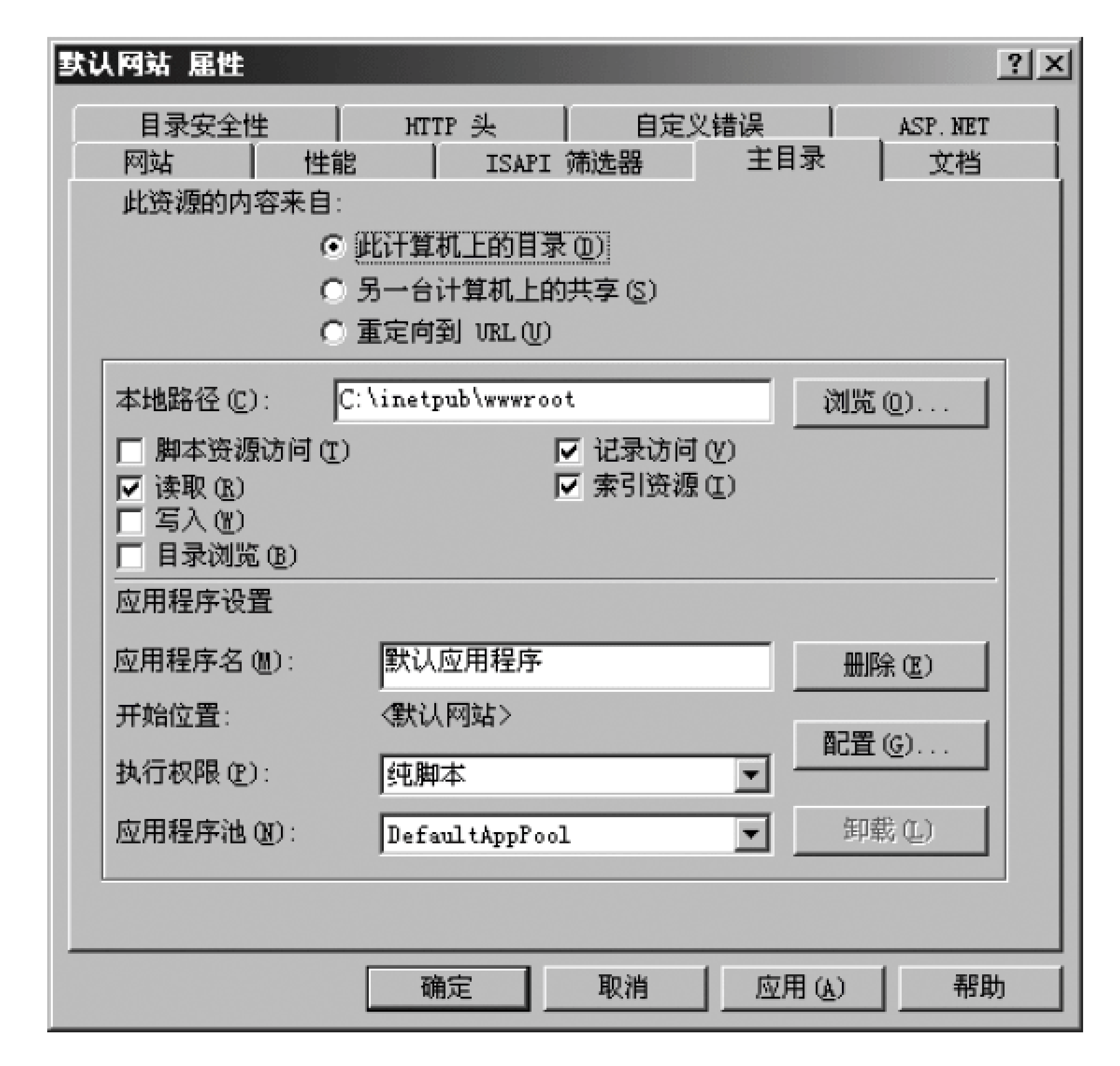


图 9-32 “主目录”选项卡

权限。

(1) 读取。客户端可以下载、浏览网页。如果 Web 站点的内容位于 NTFS 文件系统的分区上,客户端是否可以下载浏览网页还要取决于 NTFS 权限的设置。

(2) 目录浏览。允许客户端浏览 Web 站点目录。如果启用此权限,当 Web 站点没有默认文档时,客户端输入的 URL 又没有指定文件名时,浏览器显示站点的目录列表,如图 9-33 所示。但虚拟目录并不会出现目录列表中。建议不要启用目录浏览的权限,以免暴露站点内的关键信息。

```
<目录> admin
 26142 cat.asp~catid=56.html
 26105 cat.asp~catid=65.html
 19814 cat.asp~catid=82.html
 22432 cat.asp~catid=84.html
 22411 cat.asp~catid=86.html
 24399 cat.asp~catid=87.html
 17695 check.asp~ProdId=522.html
 17081 check.asp~ProdId=523.html
 16472 check.asp~ProdId=525.html
 15863 check.asp~ProdId=527.html
 15256 check.asp~ProdId=528.html
 14036 check.asp~ProdId=529.html
```

图 9-33 站点的目录列表

(3) 记录访问。将客户的访问操作记录在日志文件中。

(4) 索引资源。可以让客户端在 Web 站点的文档中快速找到所搜索的内容。

(5) 写入。允许客户端上载或编辑文件,但用户最终是否有上载或者编辑权限还要取决于这些文件的 NTFS 权限。

(6) 脚本资源访问。允许客户端访问站点脚本文件,例如 ASP、JSP 等。

在“应用程序设置”处,有“执行权限”下拉框,如图 9-34 所示。

(1) 脚本和可执行文件。允许运行任何应用程序,包括映射到脚本引擎和 Windows 二进制文件(.dll 和 .exe 文件)的应用程序。

(2) 纯脚本。在无须设置执行权限的情况下,使映射到脚本引擎的应用程序可以在此目录中运行。脚本权限比执行权限更安全。

(3) 无。不允许任何程序在 Web 站点中运行,即客户端只有浏览静态网页的权限。

默认情况下 Windows Server 2003 操作系统只能支持静态网页的访问,要想支持其

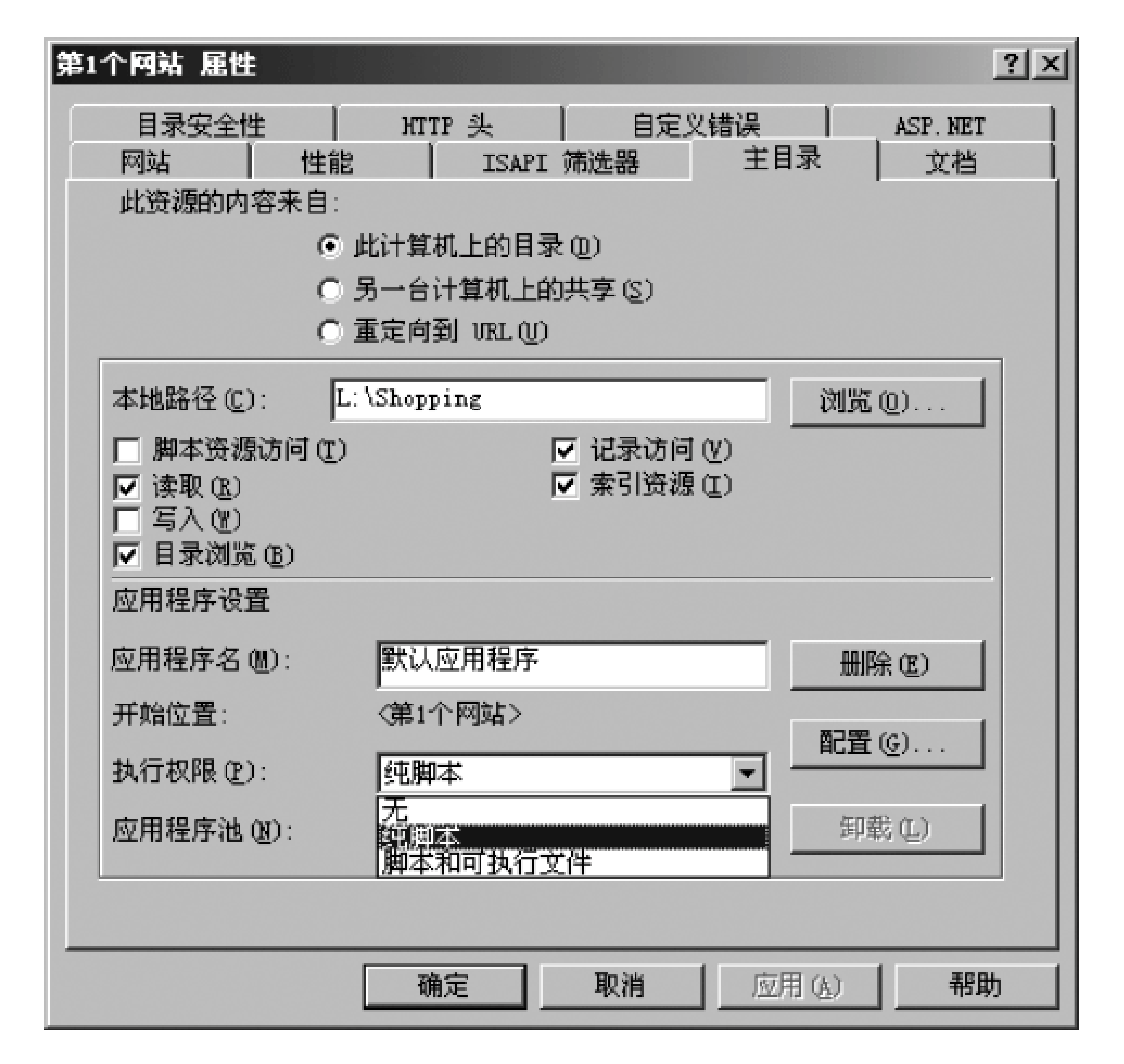


图 9-34 IIS 执行权限

他类型的动态访问网站，需要在 Web 扩展服务中自行启动相关的服务扩展，以便让 IIS 支持其他类型的网站。

要启动/禁止扩展服务，操作步骤为：启动 IIS 管理器，展开本地计算机，选择“Web 服务扩展”，如图 9-35 所示，右击要启动的服务，选择“允许”/“禁止”选项，或者在选取该服务后，单击“允许”/“禁止”按钮。

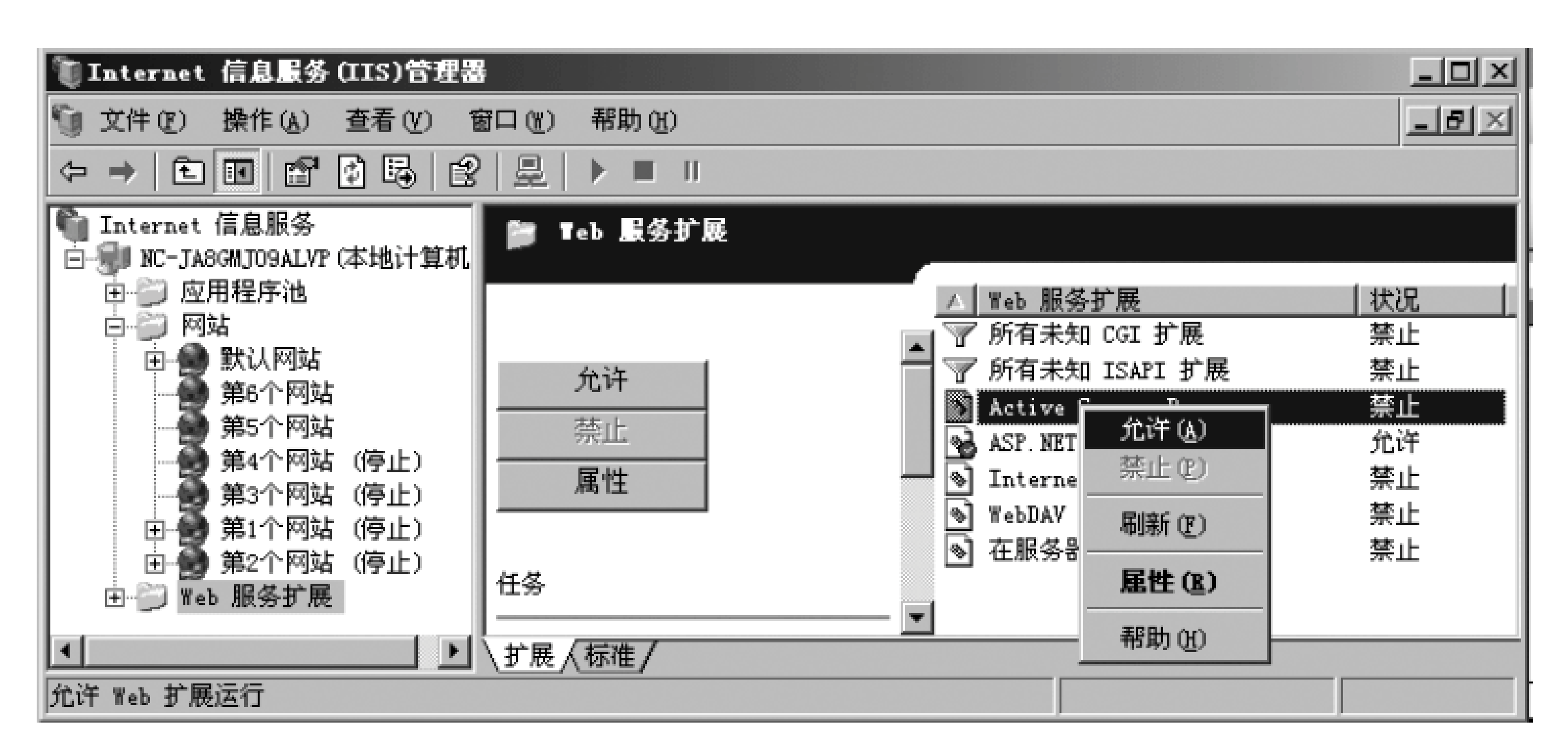


图 9-35 启动/禁止扩展服务

9.4.3 使用 NTFS 权限

要防止未经授权的用户访问站点的内容，就需要恰当而安全地配置站点内文件夹和文件的 NTFS 权限。NTFS 权限与 Web 站点的访问权限结合共同决定用户的最终权限，并采用对用户限制最严格的权限(即两者权限的交集)，以增强网站的安全性。

与 Web 站点的访问权限不同，NTFS 权限会影响通过任何方式访问网站内容（例如本地、远程访问或者通过浏览器访问）的用户，而 Web 站点的访问权限仅会影响通过浏览器访问该网站的用户。

要设置网站的文件夹或文件的 NTFS 权限，操作步骤为：右击网站的文件夹或文件，选择“属性”→“安全”选项卡，可以针对特定的用户或组设置必要的 NTFS 权限，如图 9-36 所示。

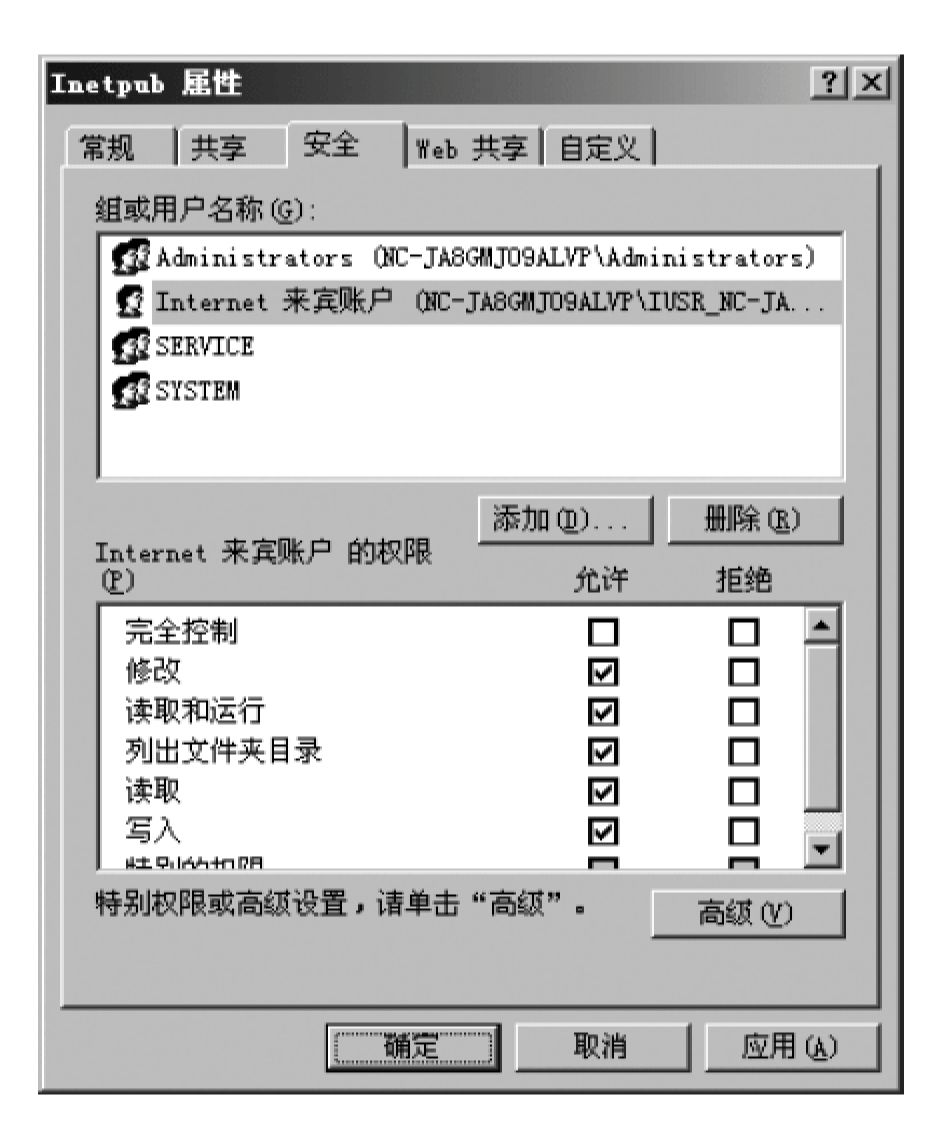


图 9-36　设置网站的文件夹的 NTFS 权限

在确保网站提供的各项内容或服务都能正常运行的情况下，要给网站的文件或文件夹设置尽可能少的 NTFS 权限，其他无用的权限都删除掉，从而保证网站内容的安全。

第 10 章　远程访问与虚拟专用网

学习目标

通过本章学习，了解连接到远程访问服务器的方式以及数据通信协议，掌握如何配置远程访问服务器，以及如何配置客户端使之能拨号连接到远程访问服务器，掌握 VPN 服务器的配置。

10.1　连接到远程访问服务器的方式

通过配置路由和远程访问(Routing and Remote Access Service，RRAS)，远程用户可以连接本地的局域网。而虚拟专用网络(Virtual Private Network，VPN)可以让远程用户通过 Internet 来安全地访问公司内部的网络资源。

1. 通过 PSTN 连接

通过 PSTN 接入是指用户利用现有的公共交换电话网(Published Switched Telephone Network，PSTN)并通过调制解调器(Modem)拨号接入到 Internet 或局域网，如图 10-1 所示。

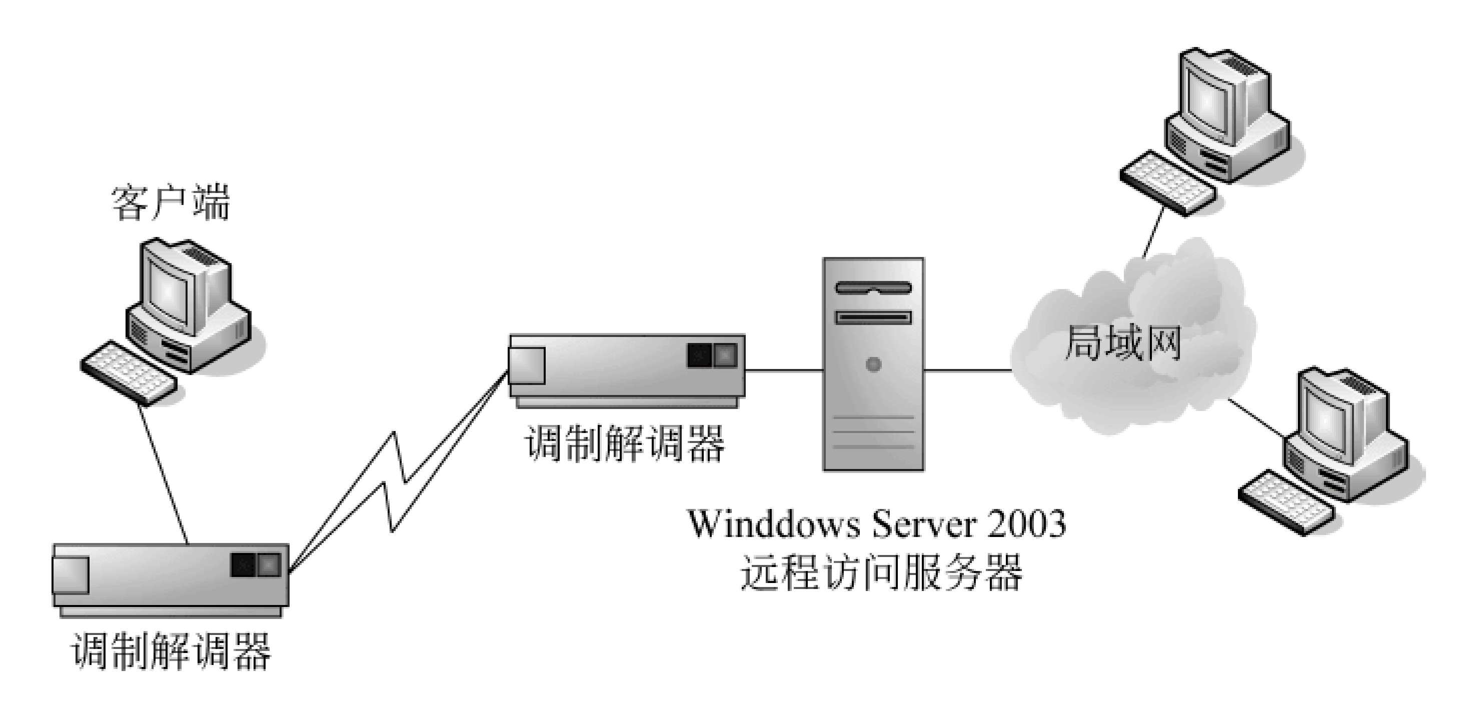


图 10-1　通过 PSTN 连接到远程访问服务器

PSTN 采用模拟信号，而计算机采用数字信号，因此客户端与服务器端之间的通信需要通过 Modem 来执行模拟信号与数字信号之间的转换。目前这种接入方式最高的速率为 56kbps，远远不能满足传输大容量信息的宽带需求，但由于电话网非常普及，Modem 又很便宜，因此这种接入方式最为经济。

2. 通过 ADSL Modem 连接

通过 ADSL Modem 实现拨号接入到 Internet 或局域网，必须确定有网卡、ADSL Modem 及配套的分离器(或称为滤波器)，如图 10-2 所示。

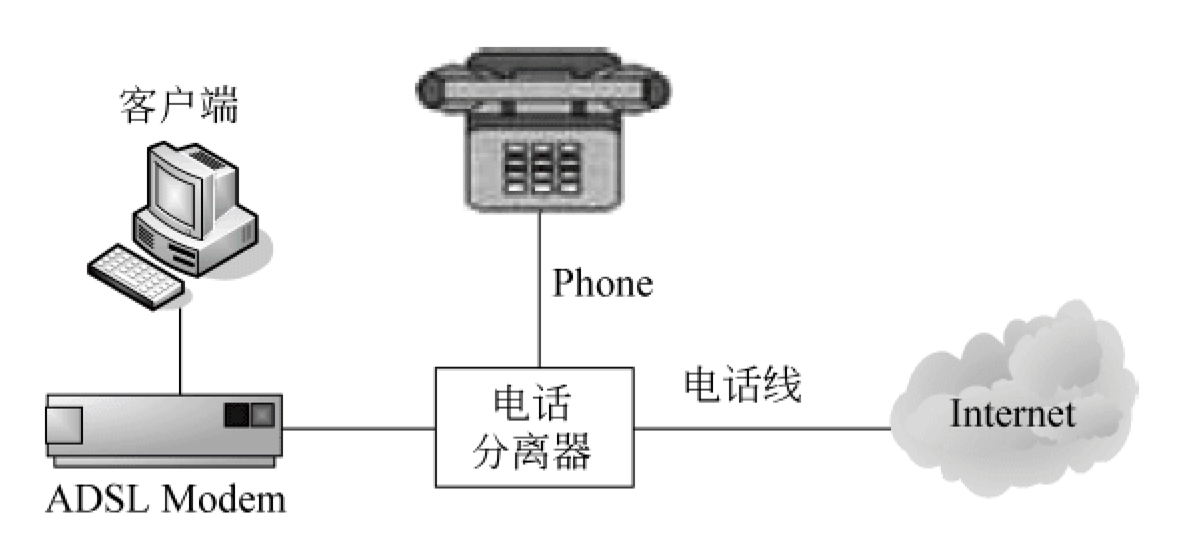


图 10-2 通过 ADSL Modem 连接到远程访问服务器

3. 直接电缆连接

直接电缆连接是指利用计算机的串行端口(COM)或并行端口(LPT)在计算机之间来实现数据的传输,有两种连接的方式。

(1) 串行端口。客户端可以直接利用一条 RS-232C 调制解调器电缆来连接远程访问服务器,这条电缆的两端分别连接到这两台计算机的 COM 端口。这种方式连接速度也较慢,并要求两台计算机之间的距离也不宜超过 15m,否则信号会失真。

(2) 并行端口。也就是通过打印机的连接端口(LPT)来连接,并要求并口电缆长度最好不超过 3m。

直接电缆连接不需要网卡,因此连接的成本低廉,但连接距离较短,传输速度较慢。

4. 通过虚拟专用网连接

虚拟专用网(Virtual Private Network,VPN)让远程用户可以通过 Internet 安全地访问公司内部的网络资源。VPN 是专用网络的延伸,通过公共网络基础设施(例如 Internet)为用户创建隧道,并提供与专用网络一样的安全功能。Windows Server 2003 支持的 VPN 通信协议有 PPTP(Point-to-Point Tunneling Protocol)与 L2TP(Layer Two Tunneling Protocol)。VPN 最大的好处是方便用户访问公司内部网络,并降低访问公司内部网络的成本。

10.2 数据传输通信协议

Windows Server 2003 远程访问网络中的客户端和服务器必须支持两类数据传输通信协议:一类是远程访问通信协议,用来控制广域网连接上的数据传输;另一类是局域网通信协议,用于控制远程客户端访问服务器及其所在网络。典型的远程访问网络的结构如图 10-3 所示。

10.2.1 远程访问通信协议

Windows Server 2003 远程访问服务器支持的远程访问通信协议有 4 个。

(1) PPP(Point-to-Point Protocol)。PPP 作为一种工业标准,是目前应用广泛的远

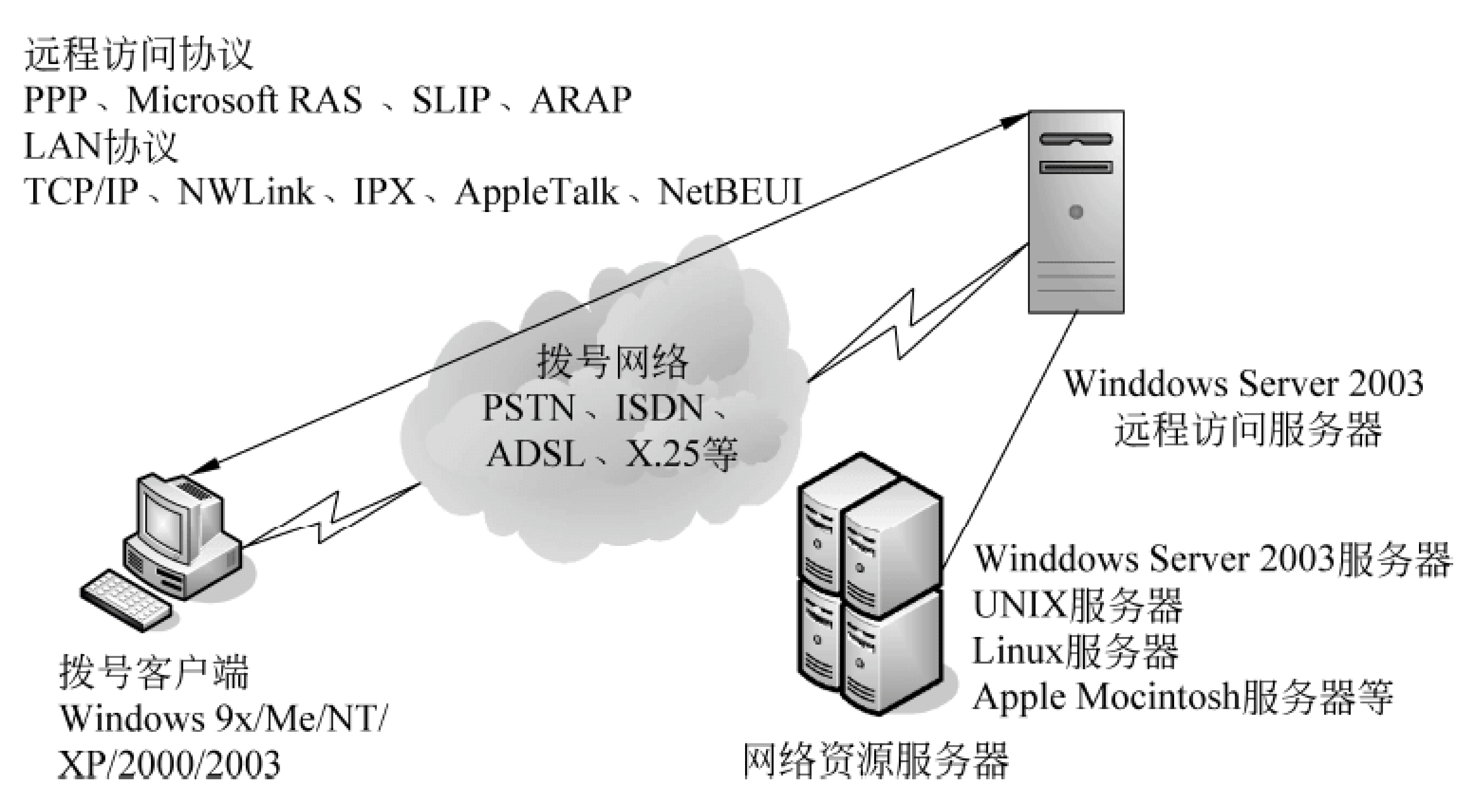


图 10-3　远程访问网络的结构

程访问通信协议，而且其安全措施完善、扩充性较强，能够满足当前与未来的需求，是微软公司推荐的远程访问协议。

(2) SLIP(Serial Line Internet Protoco1)。SLIP 全称为串行线路网际协议，主要应用在 UNIX 远程访问服务器下，作为较旧的远程访问协议，还存在一些问题。Windows Server 2003 远程访问服务器不支持客户端利用 SLIP 来连接，但是 Windows NT、Windows XP、Windows 2000 等远程访问客户端支持 SLIP，可以连接到符合 SLIP 标准的远程访问服务器。

(3) ARAP(AppleTalk Remote Access Protocol)。该协议支持 Apple 的 Macintosh 远程访问客户端连接到 Windows Server 2003 远程访问服务器，但 Windows Server 2003 远程访问客户端不支持利用 ARAP 来连接支持 ARAP 的远程访问服务器。

(4) Microsoft RAS Protocol(Microsoft Remote Access Service Protocol)。该协议是微软公司专有的数据传输通信协议，是早期 Windows 操作系统所广泛采用的专用远程访问通信协议，只能配合 NetBEUI 局域网通信协议使用，因此远程访问服务器和客户端都必须安装 NetBEUI 局域网通信协议。

10.2.2　局域网通信协议

客户端利用远程访问通信协议连接到远程访问服务器后，需要再利用局域网通信协议与远程访问服务器通信，并通过远程访问服务器与局域网内的其他计算机通信。Windows Server 2003 远程访问支持的局域网通信协议有 TCP/IP、NWLink、IPX/SPX、AppleTalk 和 NetBEUI 等。局域网通信协议可以限制远程访问客户端是访问整个网络还是只能访问远程访问服务器本身。

10.3　远程访问网络

Windows Server 2003 集成了远程访问服务组件，效率虽然不如专门的硬件设备，但在有些场合下不失为一种经济、有效的解决方案，特别适合远程接入用户较少的网络

使用。

在图 10-4 所示的远程访问网络中，客户端通过调制解调器拨号连接到 Windows Server 2003 远程访问服务器。要实现从客户端连接到远程访问服务器，需要完成以下三步。

(1) 安装远程访问服务器。

(2) 授予用户远程访问的权限。

(3) 客户端的设置。

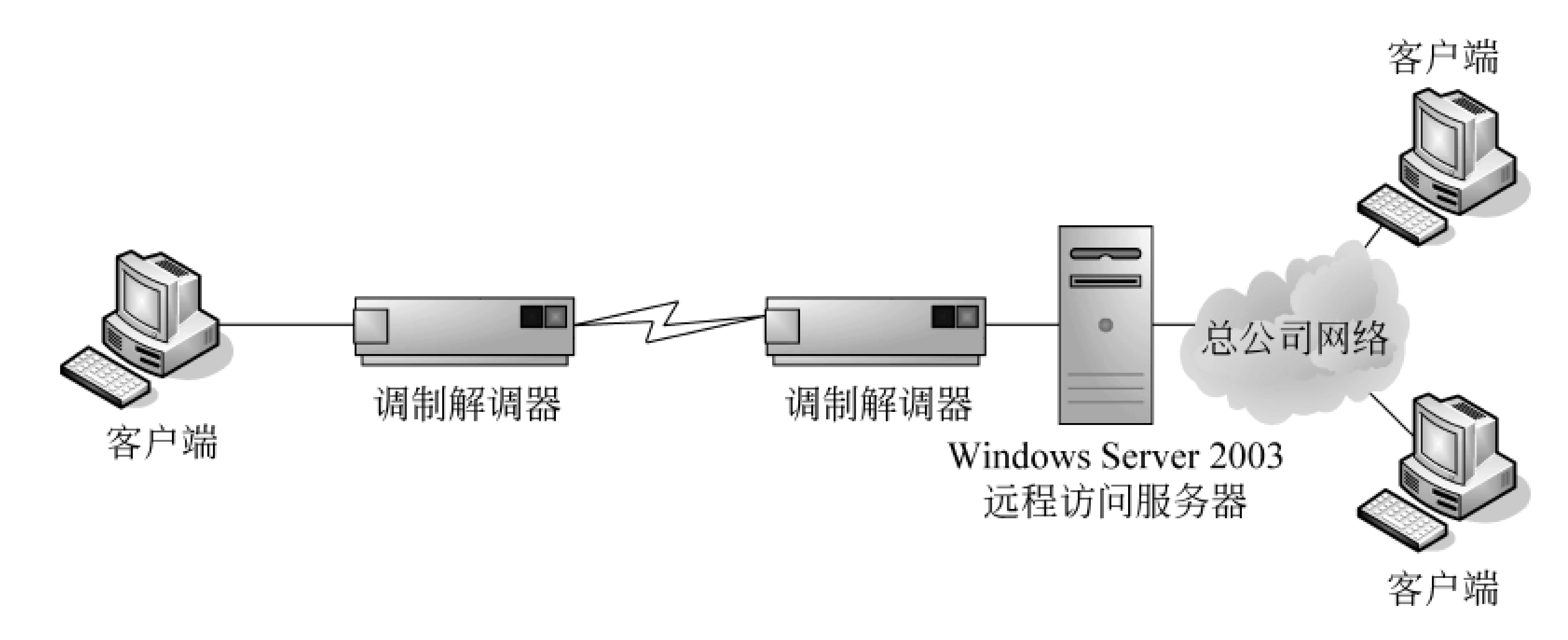


图 10-4 远程访问网络

10.3.1 安装远程访问服务器

要配置 Windows Server 2003 远程访问服务器，服务器上要事先安装调制解调器。如果 Windows Server 2003 服务器启用了"Internet 连接防火墙(Internet Connection Firewall，ICF)"，请先停用 ICF，否则无法安装远程访问服务器。

安装远程访问服务器的操作步骤如下。

(1) 打开"路由和远程访问"控制台，右击 SERVER01(本地)，在弹出的快捷菜单中选择"配置并启用路由和远程访问"选项，如图 10-5 所示。

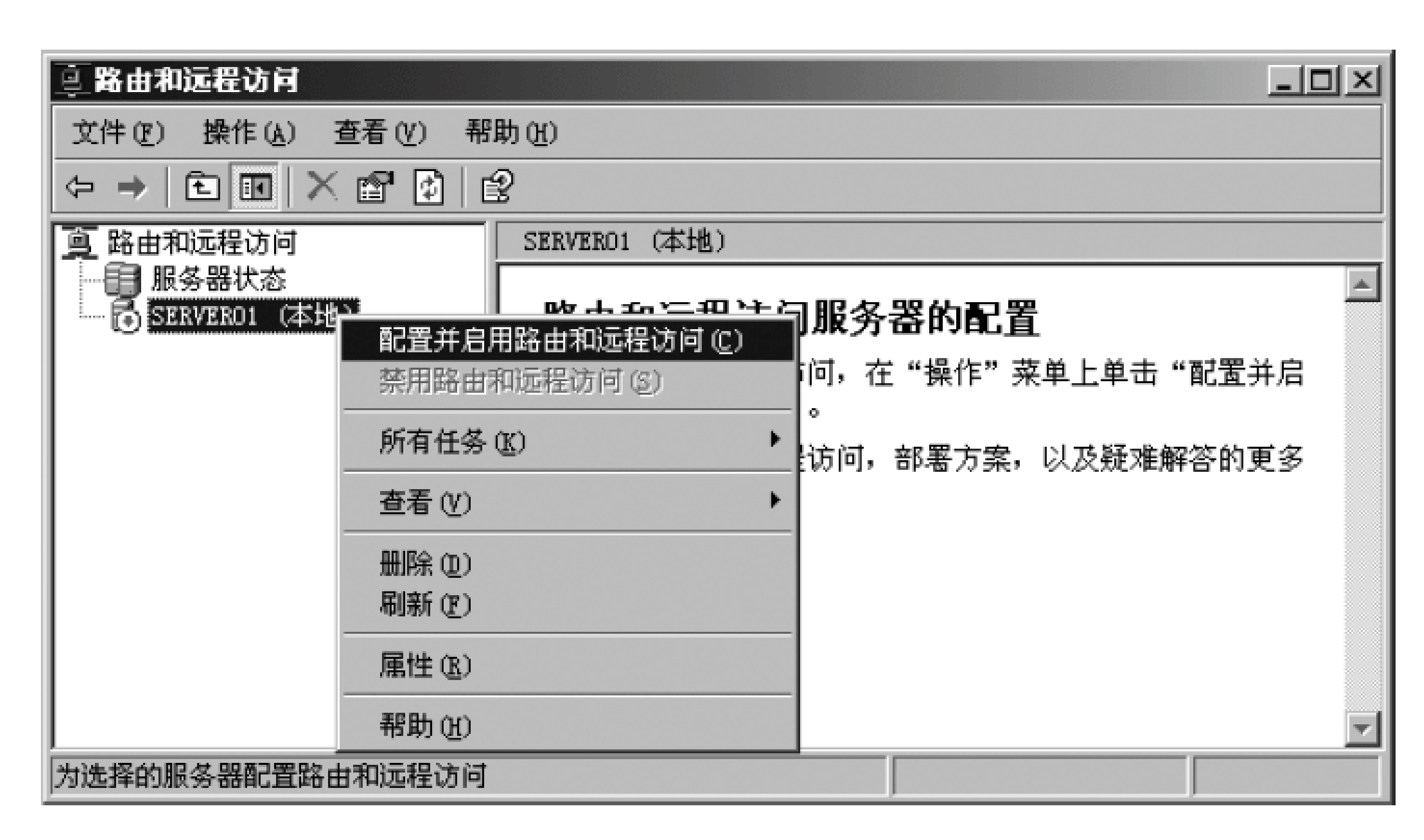


图 10-5 配置并启用路由和远程访问

(2) 在“欢迎使用路由和远程访问服务器安装向导”对话框中，单击“下一步”按钮。在图 10-6 中，选择“远程访问(拨号或 VPN)”单选按钮，单击“下一步”按钮。

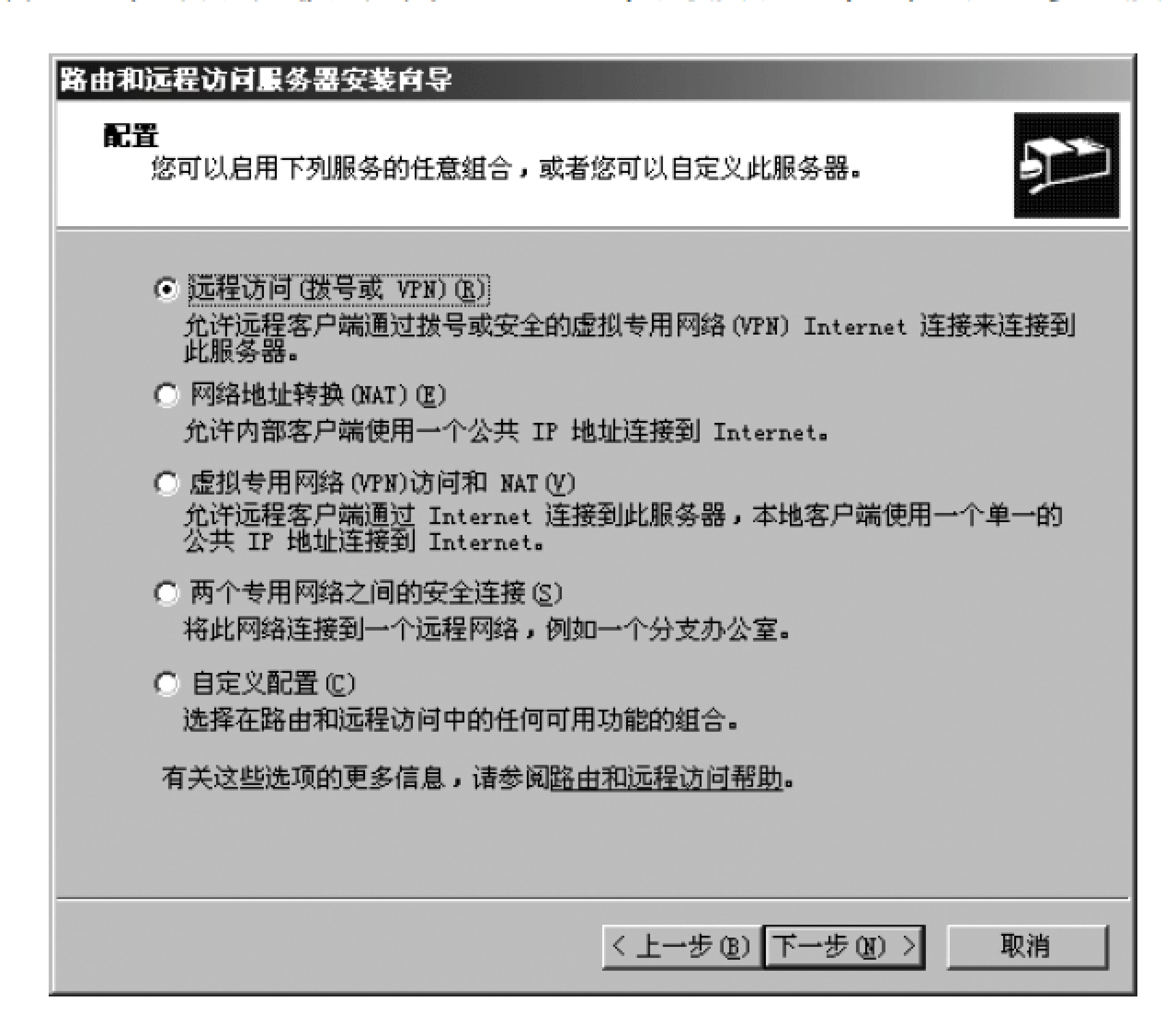


图 10-6　选择“远程访问(拨号或 VPN)”单选按钮

(3) 在图 10-7 中，选中“拨号”复选框，单击“下一步”按钮。

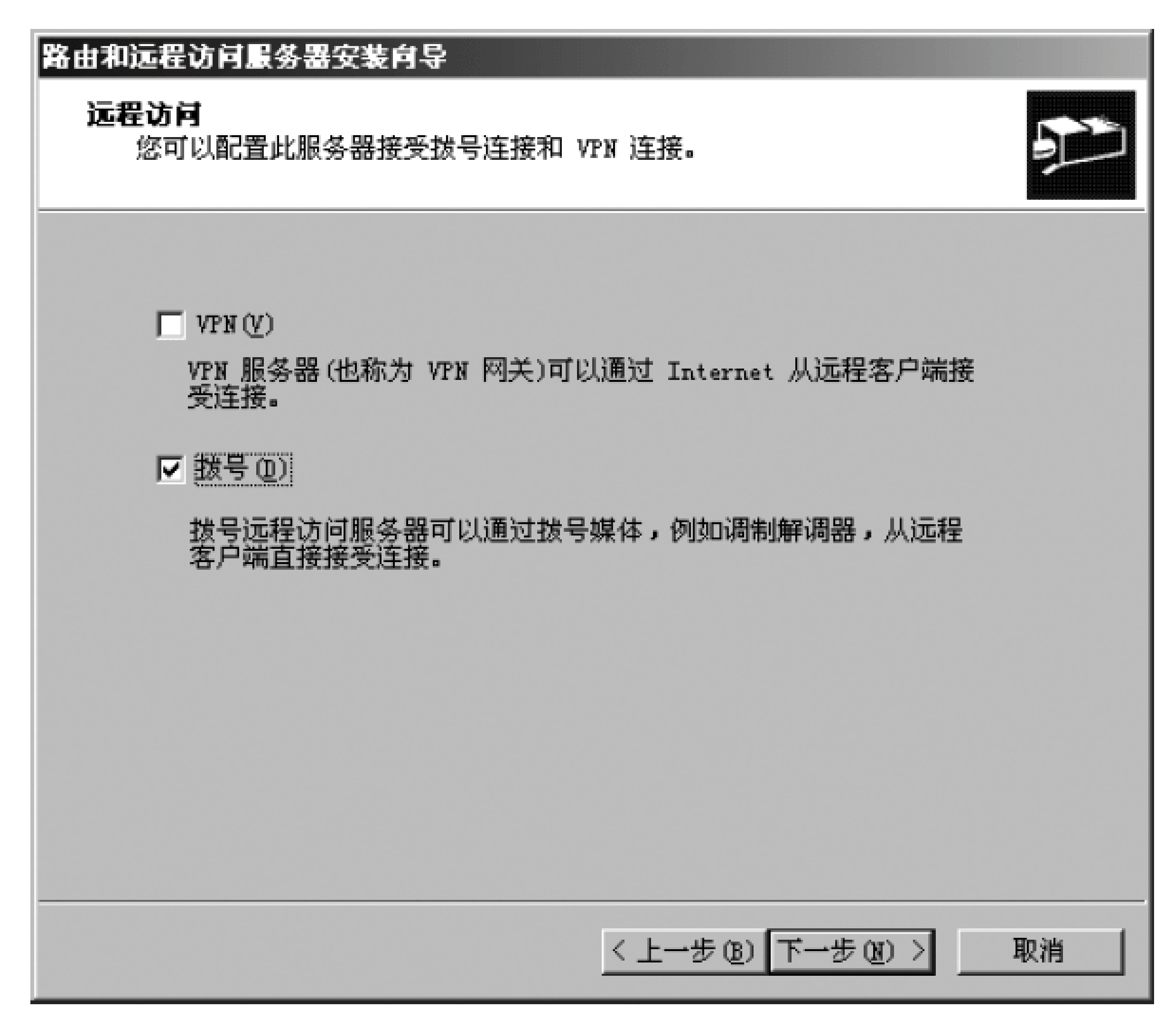


图 10-7　选中“拨号”复选框

(4) 若该服务器安装了多个网卡，每一个网卡连接到一个网络，此处要设置当客户端拨号连接成功后将属于哪一个网络，以便为该客户端分配 IP 地址。在此选择“本地连接”，如图 10-8 所示，单击“下一步”按钮。

(5) 在图 10-9 中，选择为客户端指派 IP 地址的方法。可以利用 DHCP 服务器自动

分配，也可以定义一个 IP 地址池。在此选择“自动”单选按钮，单击“下一步”按钮。

路由和远程访问服务器安装向导

网络选择

您可以将远程客户端指派到您想让他们使用的网络。

由于寻址，拨号访问和其它原因，远程客户端必须被指派到一个网络。请从下面的列表中选择一个合适的网络连接。

网络接口(I):

名称	描述	IP 地址
本地连接	Realtek RTL8139 F...	59.70.142.248
本地连接2	VMware Virtual Et...	202.196.0.1

< 上一步(B) 下一步(N) > 取消

图 10-8 指派客户端所属的网络

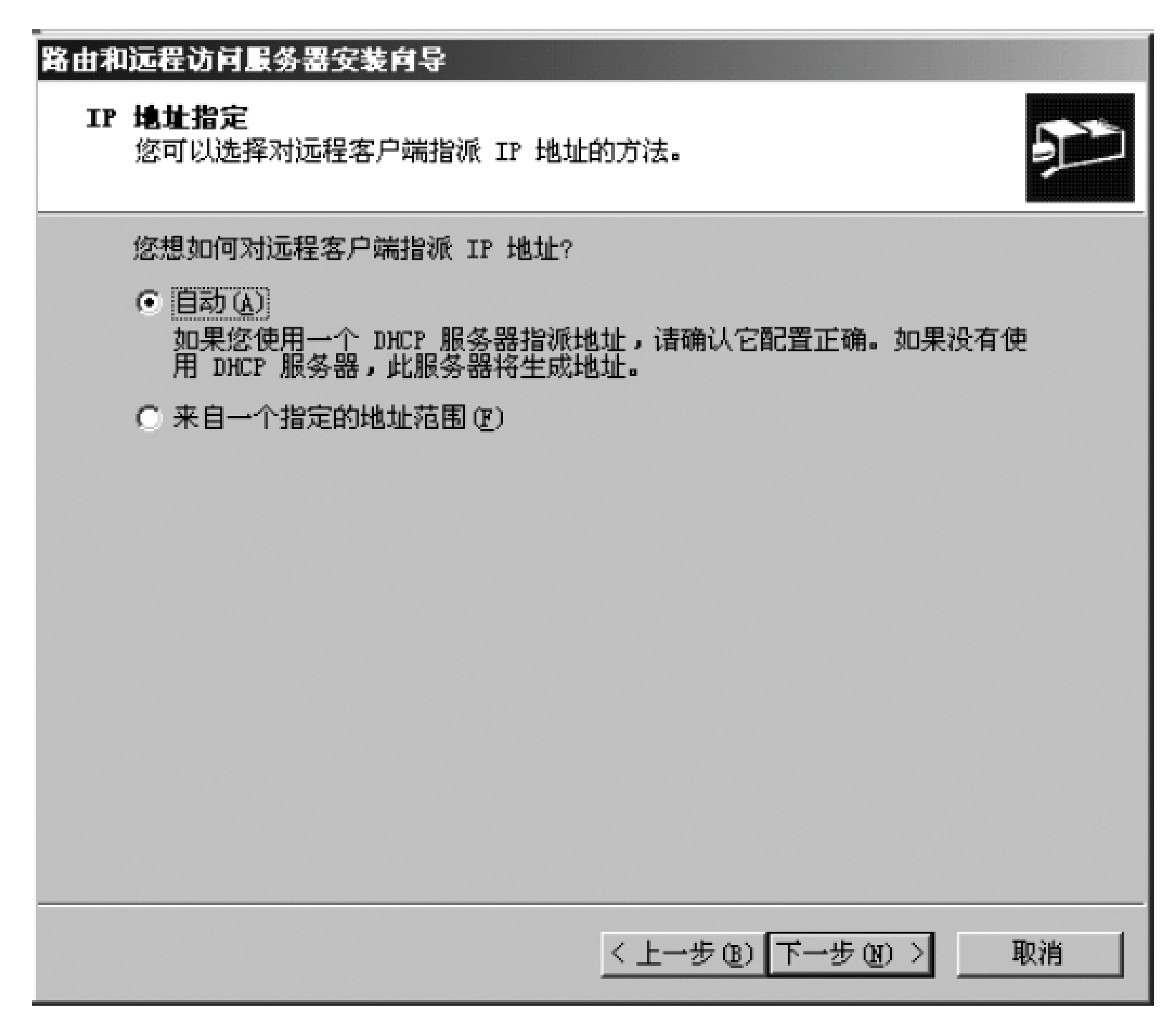


图 10-9 选择为客户端指派 IP 地址的方法

(6) 在图 10-10 中，选择“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮，单击“下一步”按钮。

(7) 再出现“完成路由和远程访问服务器安装向导”对话框时，单击“完成”按钮。出现图 10-11 时，单击“确定”按钮。

(8) 远程访问服务器安装完成后，如图 10-12 所示。若要将远程访问客户端的 DHCP 消息转发到其他网络内的 DHCP 服务器，在“IP 路由选择”下的“DHCP 中继代理

程序”中进行设置。

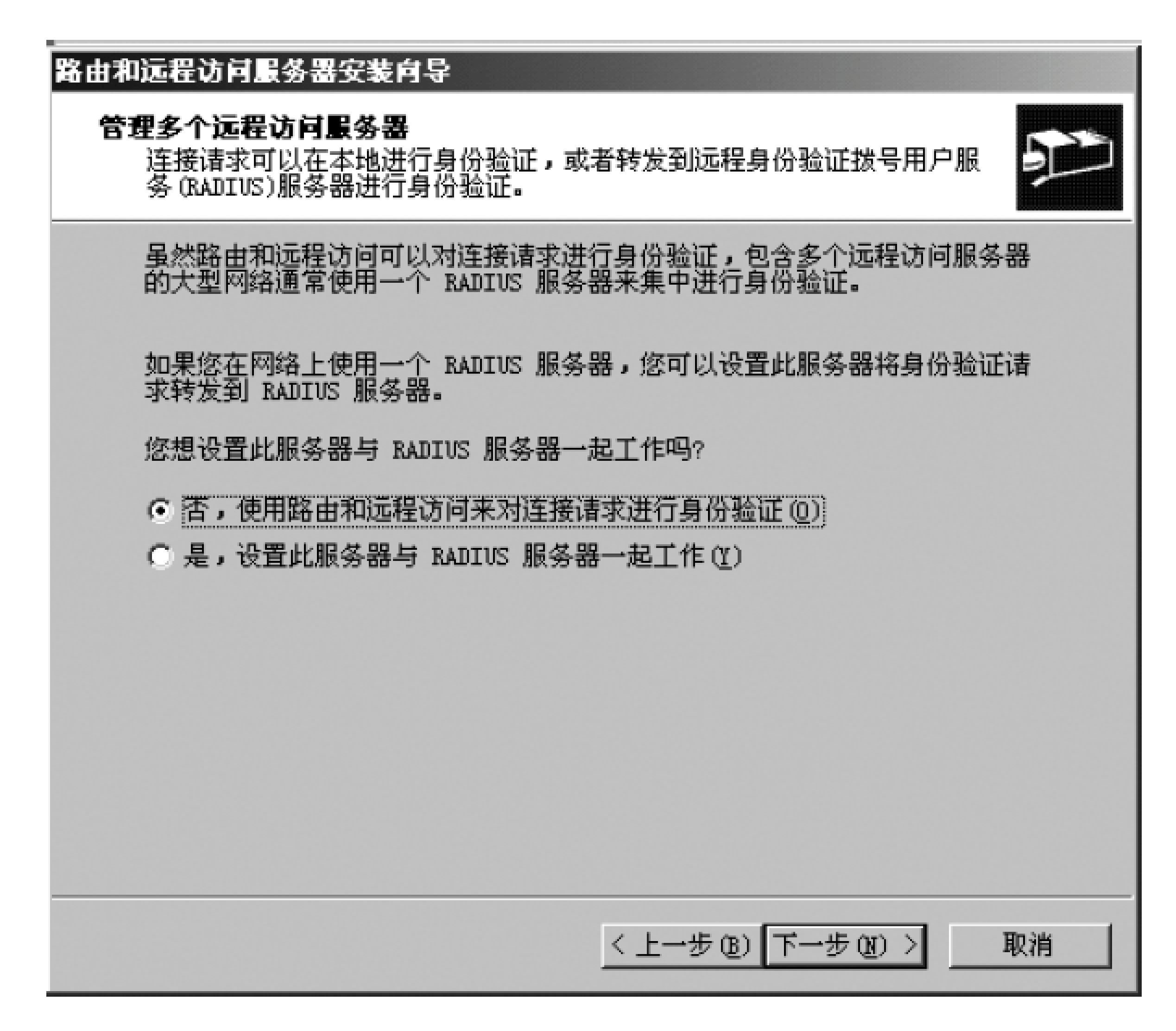


图 10-10　管理多个远程访问服务器

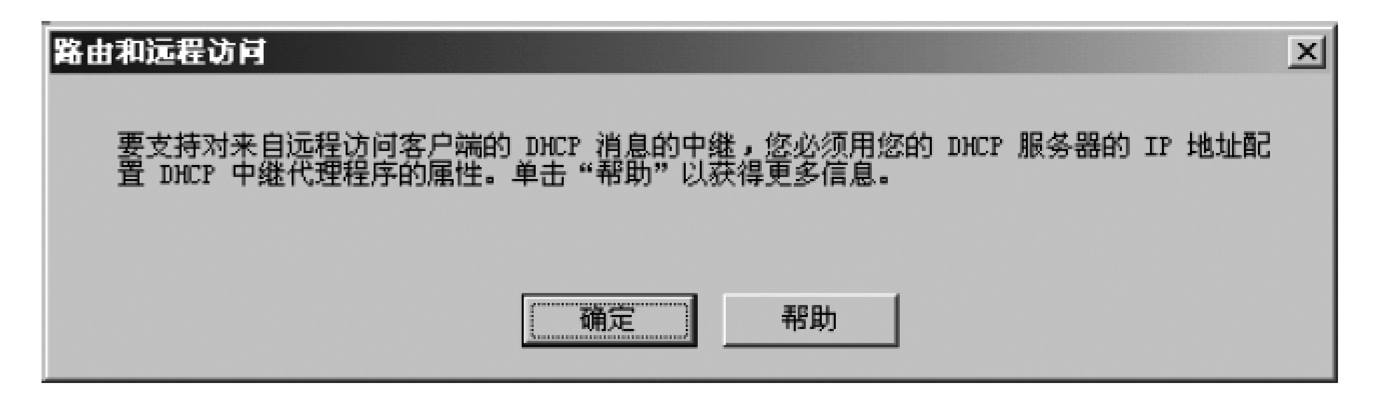


图 10-11　路由和远程访问消息框

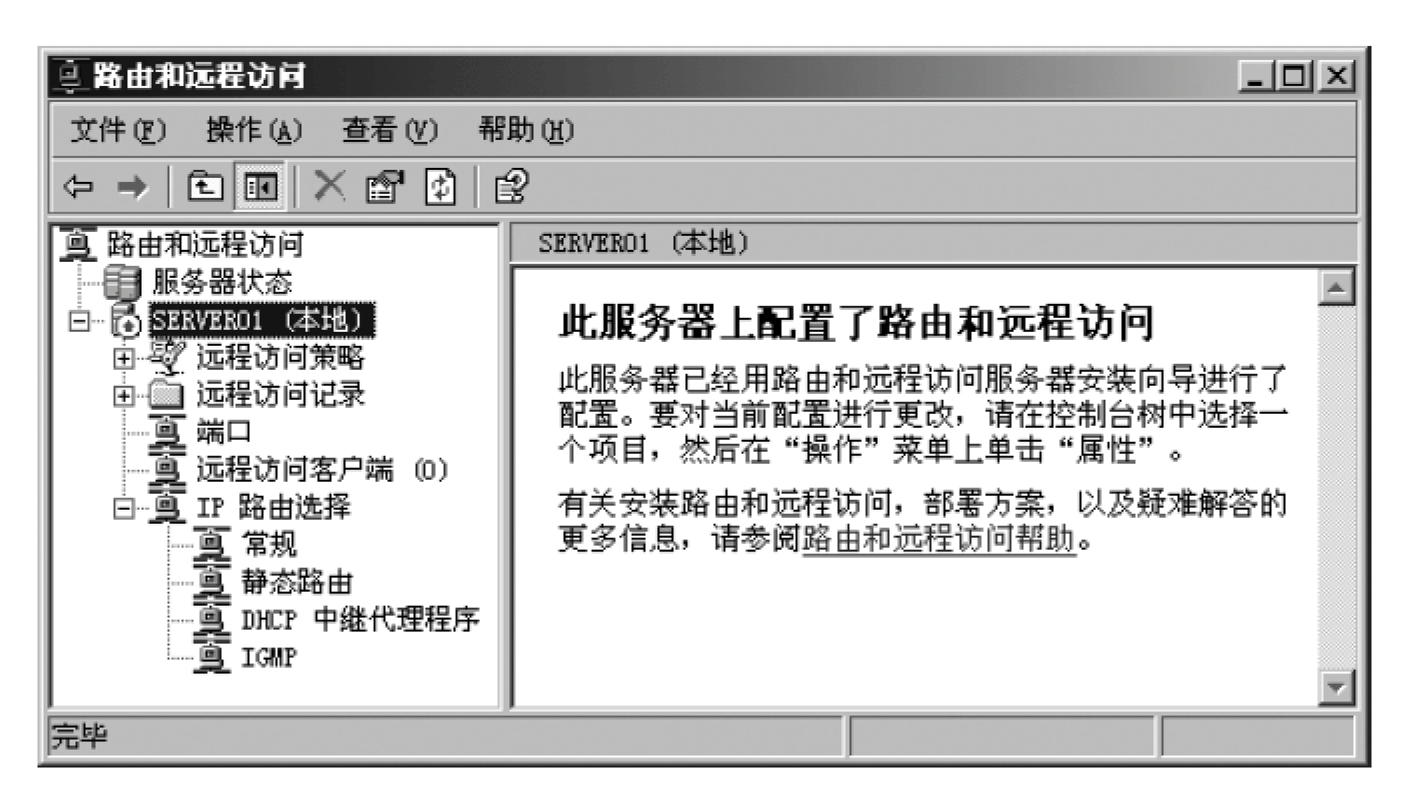


图 10-12　远程访问服务器安装完成后

在远程访问客户端成功建立拨号连接后，若要限制客户端只能访问这台远程访问服务器内的资源，而不能访问远程访问服务器所在网络内其他计算机的资源，操作步骤为：右击图 10-5 中的 SERVER01(本地)→选择“属性”命令→“IP”选项卡，去掉“启用 IP 路

由”前的复选框即可。

10.3.2 授予用户远程访问的权限

默认情况下，域用户账户或本地用户账户都没有拨号连接到远程访问服务器的权限。要使这些用户能够和远程访问服务器建立连接，必须为这些用户授予拨入权限，并且这些用户账户的密码均不能为空，否则拨入验证不会成功。

1. 授予域用户远程访问的权限

要授予域用户远程访问的权限，操作步骤为：单击“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”，右击要设置的用户账户→“属性”→“拨入”选项卡，打开图 10-13，在“远程访问权限(拨入或 VPN)”区域选中“允许访问”单选按钮，然后单击“确定”按钮即可。

2. 授予本地用户远程访问的权限

要授予本地用户远程访问的权限，操作步骤为：单击“开始”→“程序”→“管理工具”→“计算机管理”→“本地用户和组”→“用户”，右击要设置的用户账户→“属性”→“拨入”选项卡，打开图 10-14，在“远程访问权限(拨入或 VPN)”区域选中“允许访问”单选按钮，单击“确定”按钮即可。

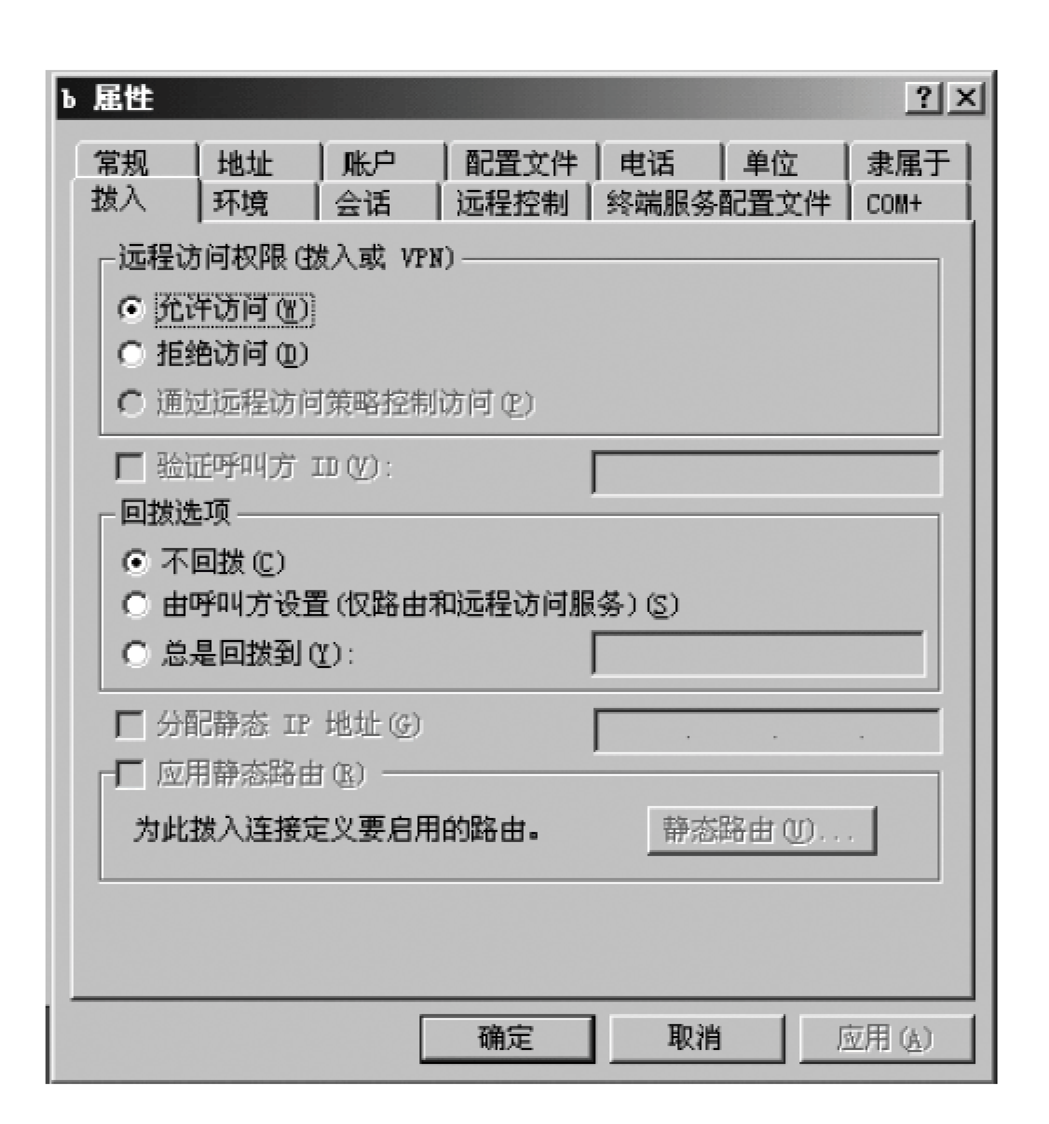


图 10-13　授予域用户远程访问的权限

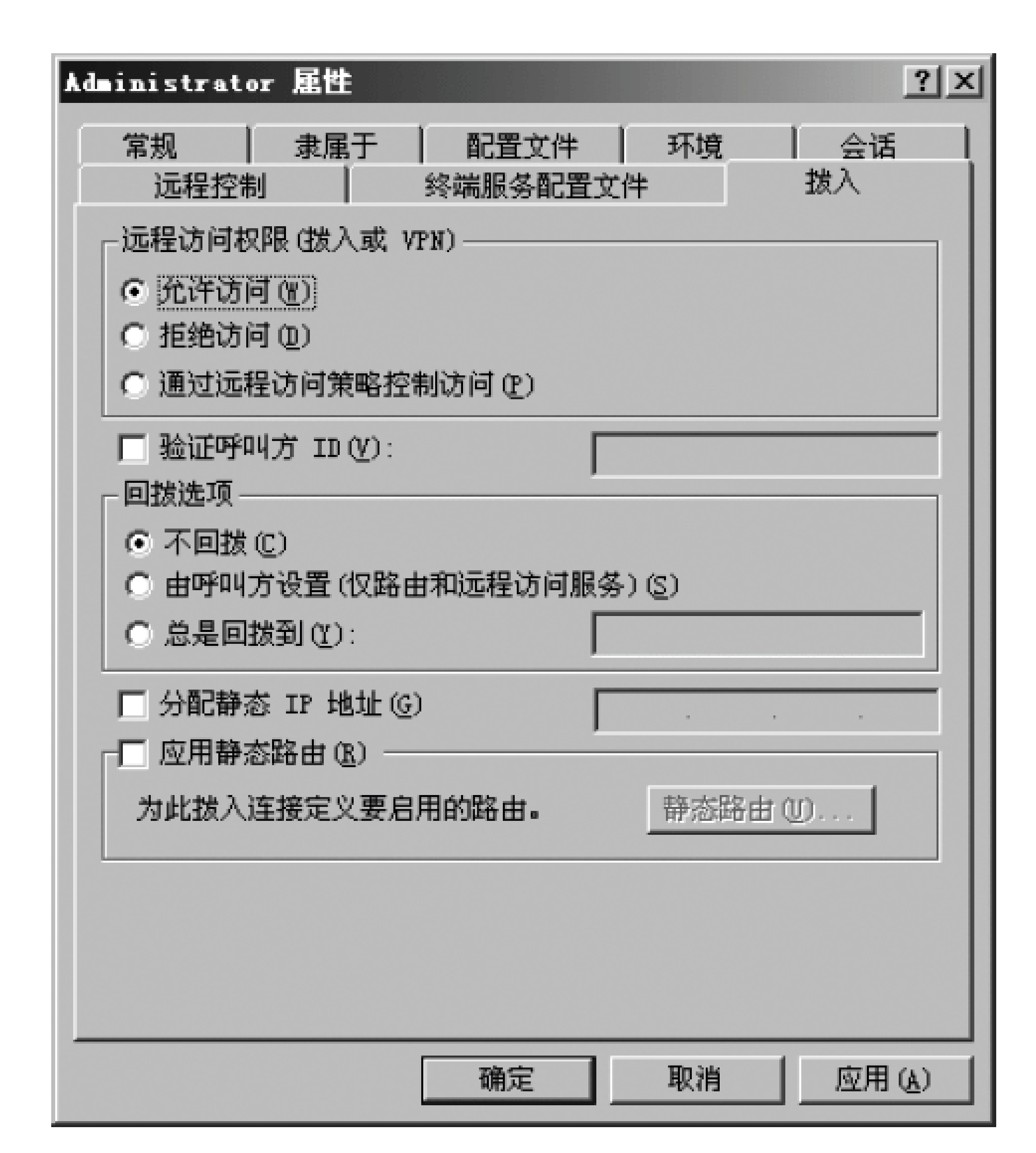


图 10-14　授予本地用户远程访问的权限

10.3.3 设置客户端

连接到 Windows Server 2003 远程访问服务器上的拨号客户端可以是 Windows Server 2003、Windows NT、Windows 2000、Windows XP 等客户端。这些客户端必须安装拨号设备(如调制解调器),配备拨号线路(如模拟电话线或其他 WAN 连接)。

以 Windows Server 2003 为例,设置远程访问客户端的操作步骤如下。

(1) 右击“网上邻居”→“属性”→“创建一个新的连接”,出现“欢迎使用新建连接向导”对话框,单击“下一步”按钮。

(2) 在图 10-15 中,选择“连接到我的工作场所的网络”单选按钮,单击“下一步”按钮。

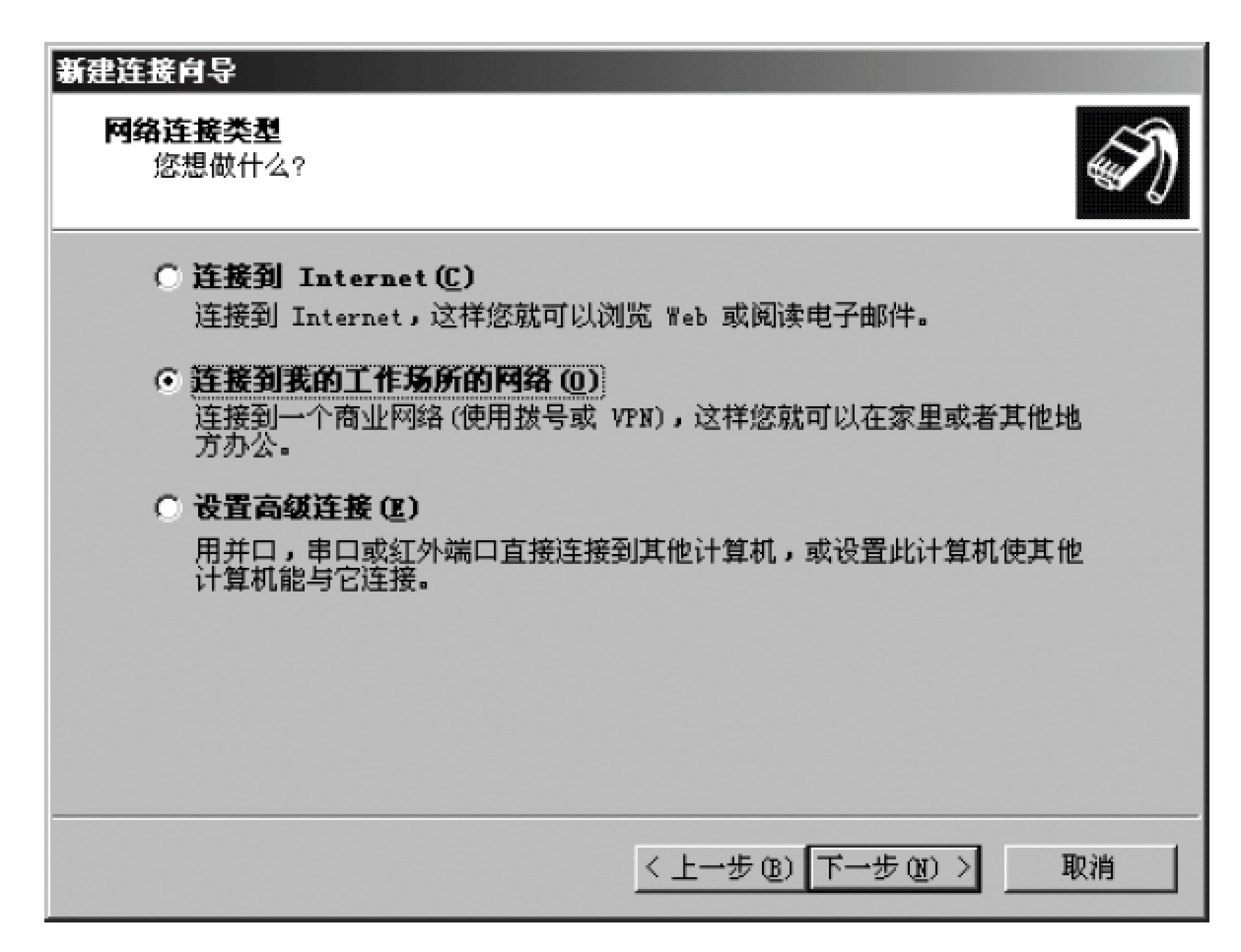


图 10-15 网络连接类型

(3) 在图 10-16 中,选择“拨号连接”单选按钮,单击“下一步”按钮。

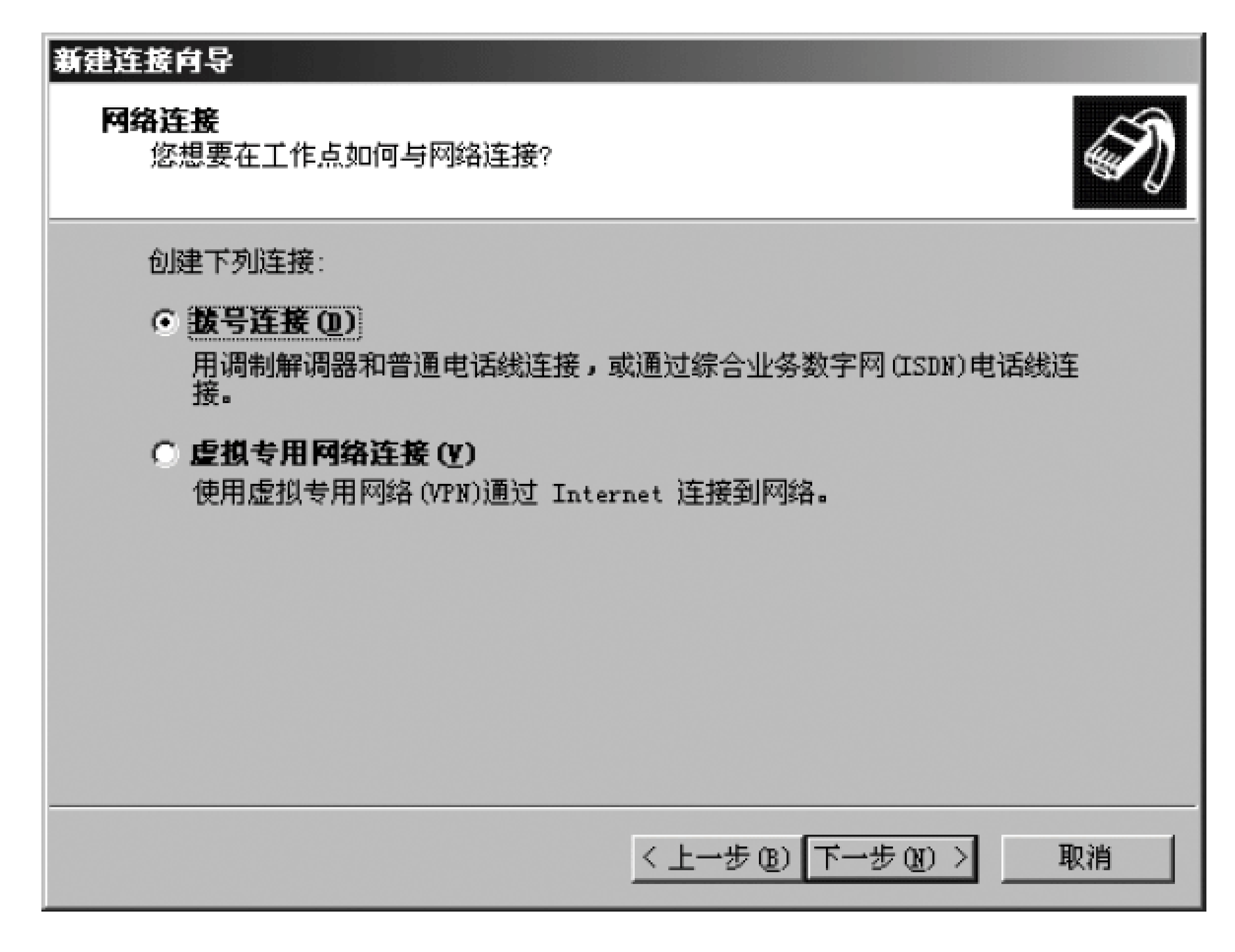


图 10-16 指定如何与网络连接

(4) 如果计算机内只安装了一个调制解调器,则系统会自动选择此调制解调器,但如果安装了多个调制解调器,则需选中其中一个调制解调器前面的复选框,如图 10-17 所示,单击"下一步"按钮。



图 10-17 选择用来建立连接的设备

(5) 在图 10-18 中,输入公司名,例如"总公司信息中心",单击"下一步"按钮。

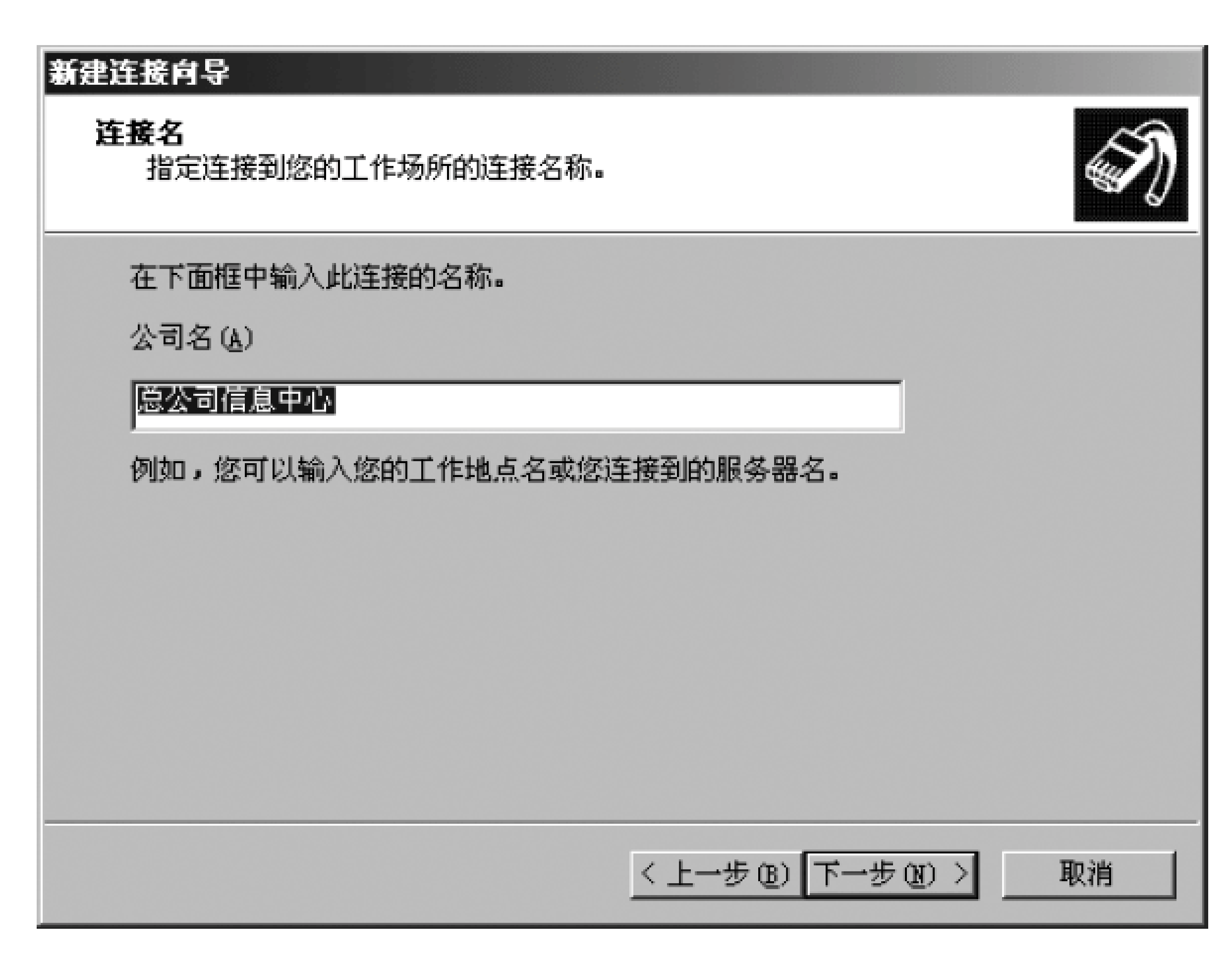


图 10-18 指定连接的名称

(6) 在图 10-19 中,输入远程访问服务器的电话号码。如果要拨外地的远程访问服务器,则需在电话号码前加区号,例如 037163556635,其中的 0371 代表河南郑州,单击"下一步"按钮。

(7) 在图 10-20 中,选择"任何人使用"单选按钮表示登录到这台计算机的所有用户都可以使用,选择"只是我使用"单选按钮表示只有建立连接的用户才可以使用。

(8) 出现"完成新建连接向导"对话框时,单击"完成"按钮即可。

为了便于访问远程服务器,可以在桌面上新建一个远程连接的快捷方式。客户端用

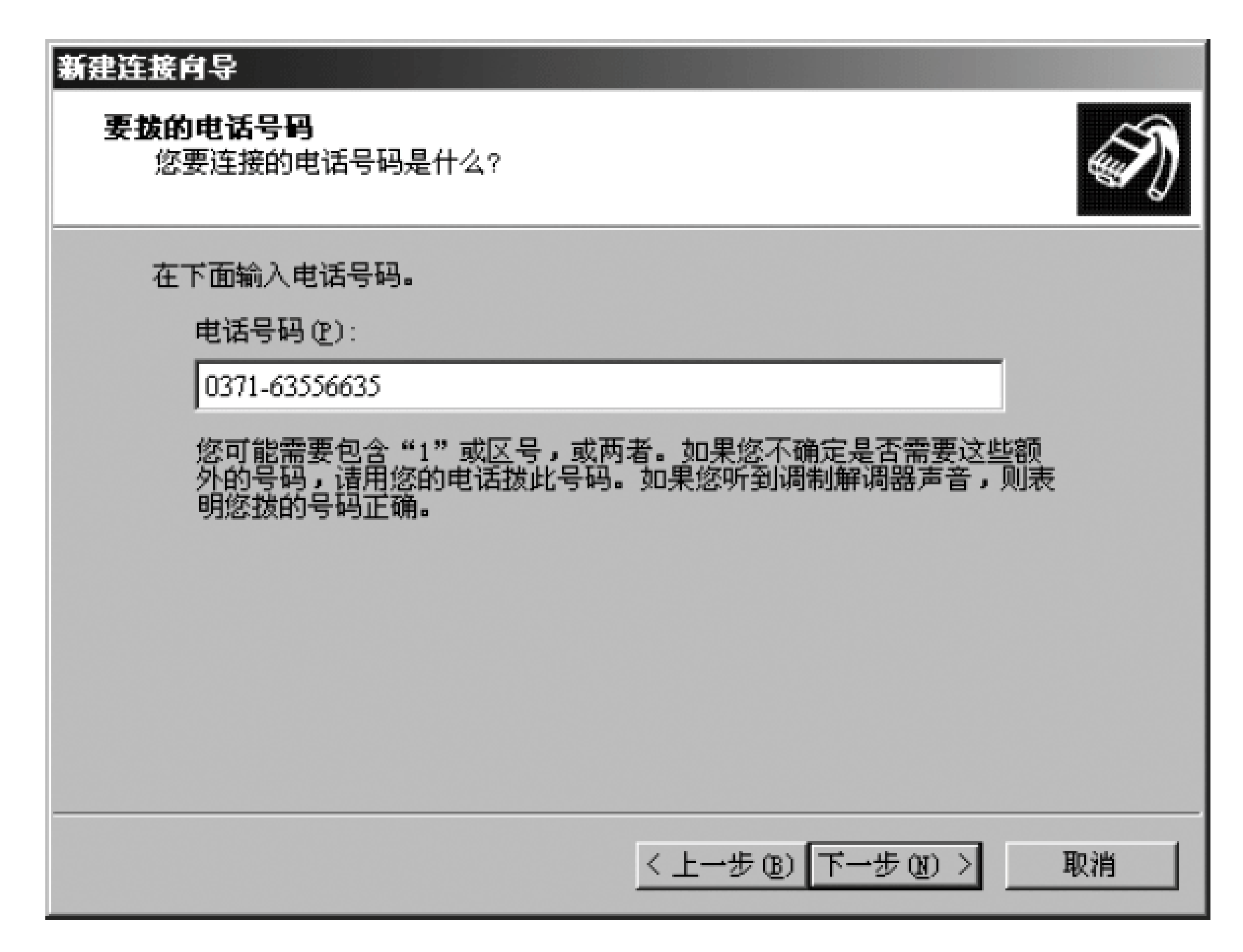


图 10-19　要拨的电话号码

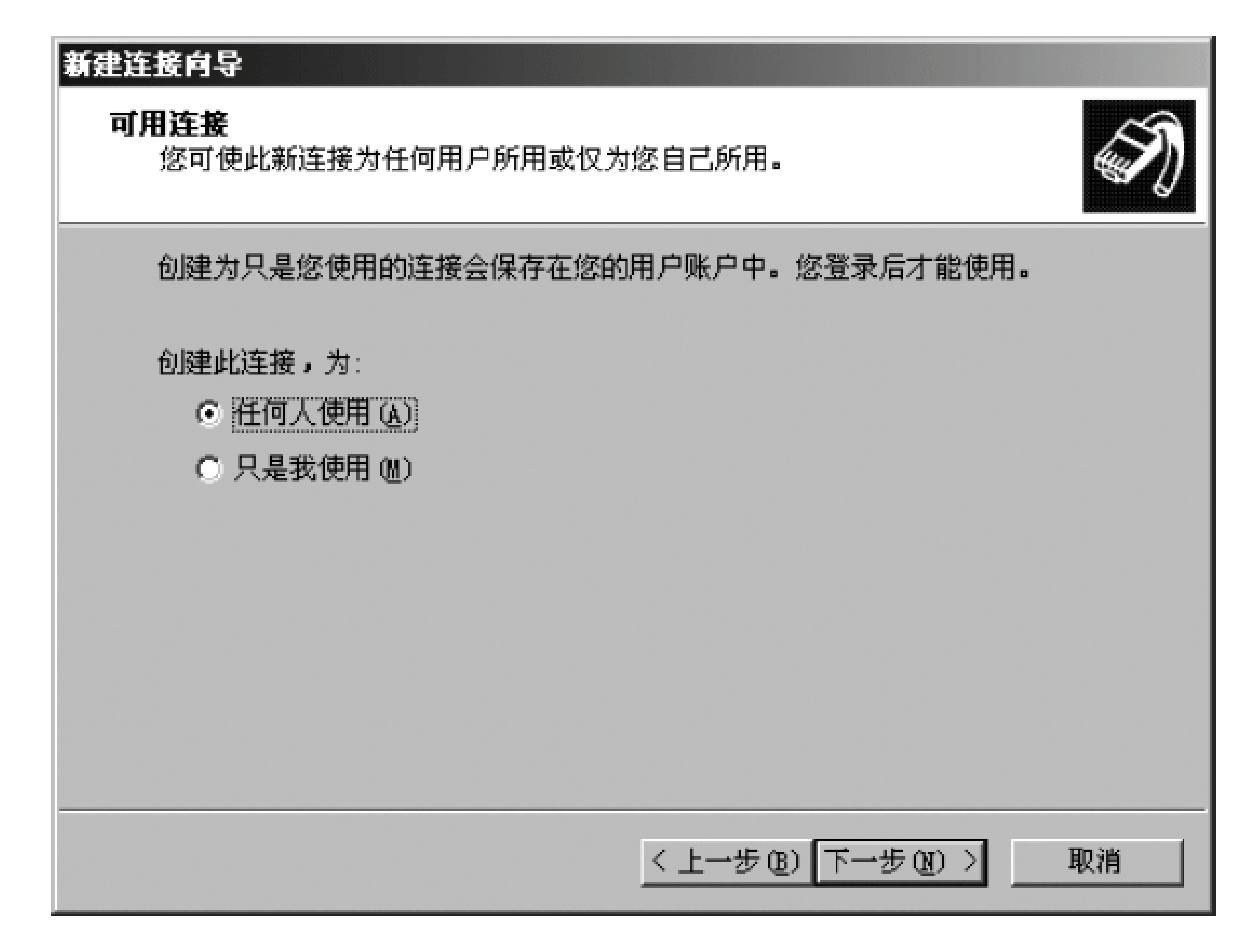


图 10-20　可用连接

户要使用刚才创建的拨号连接拨号到远程访问服务器，可以通过右击“网上邻居”，在弹出的快捷菜单中选择“属性”选项，双击创建的拨号连接的快捷方式，或是通过桌面上的快捷方式，打开“登录”对话框，输入连接远程访问服务器的用户名与密码，完成后单击“拨号”按钮即可。

10.4　虚拟专用网络

越来越多的企业通过接入 Internet，实现位于各地的分公司的内部网络互通，达到信息资源的共享，但是传输的这些数据有很多是属于内部机密，因此有必要采取一些措施来保障这些数据的安全。虚拟专用网络(Virtual Private Network，VPN)通过特定的加密协议，使位于不同地方的多个内部网之间利用现有公共网络基础架构(例如 Internet)通

过隧道技术实现数据的安全传输。

10.4.1 VPN 的工作原理

Windows Server 2003 服务器利用自带的 VPN 服务组件,使远程用户通过 Internet 等公共网络与某个局域网之间建立一条安全的通信隧道。

1. 两种 VPN 通信协议

Windows Server 2003 服务器支持以下两种 VPN 通信协议。

(1) 点对点隧道协议(Point-to-Point Tunneling Protocol,PPTP)。PPTP 是对点对点协议(PPP)的一种扩展,而 PPTP 隧道实质上是基于 IP 网络的 PPP 连接。两个局域网之间若通过 PPTP 来连接,则两个局域网的 VPN 服务器必须安装 TCP/IP,但局域网内的其他计算机不一定要安装 TCP/IP,可以安装 IPX 和 NetBEUI 等通信协议。当位于不同局域网络的远程计算机之间通过 VPN 方式通信时,这些不同局域网协议的数据包将被封装在 PPP 数据包内,然后再在现有的网络上传送,当数据到达目标网络后,再由目标网络内的 VPN 服务器将其解除封装,还原为 TCP/IP、IPX 和 NetBEUI 的数据包。

PPTP 采用了 PPP 所提供的身份验证、压缩与加密机制,PPTP 随 TCP/IP 一起自动安装。PPTP VPN 服务利用 Microsoft 端对端加密(Microsoft Point-to-Point Encryption, MPPE)对数据进行封装与加密。

(2) 第二层隧道协议(Layer Two Tunneling Protoco1,L2TP)。L2TP 是一种工业标准的 Internet 隧道协议,功能大致和 PPTP 协议类似,同样可以对数据进行加密。不同之处在于 PPTP 要求网络为 IP 网络,L2TP 要求面向数据包的点对点连接;PPTP 使用单一隧道,L2TP 使用多隧道;L2TP 提供包头压缩、隧道验证,而 PPTP 不支持。L2TP 与 IPSec 的结合称为 L2TP/IPSec;VPN 客户端与 VPN 服务器都必须支持 L2TP 和 IPSec。

2. VPN 应用的场合

一般来说,VPN 应用在以下两种场合。

(1) 总公司的网络已经连接到 Internet,在外地出差的员工拨号到当地的 ISP 接入到 Internet,然后通过 Internet 与总公司的 VPN 服务器建立 PPTP 或 L2TP 的 VPN 连接,并在 VPN 客户端与总公司的网络之间安全地传输数据。网络结构如图 10-21 所示。

(2) 两个局域网的 VPN 服务器都连接到 Internet,两个局域网内的计算机之间可以建立 PPTP 或 L2TP 的 VPN 连接,实现在两个网络之间安全地传输数据。网络结构如图 10-22 所示。

10.4.2 PPTP VPN

以图 10-23 所示的网络结构为例,介绍如何通过 Internet 在客户端与公司网络之间建立 PPTP VPN 连接。在 Windows Server 2003 VPN 服务器上安装了两块网卡,一块

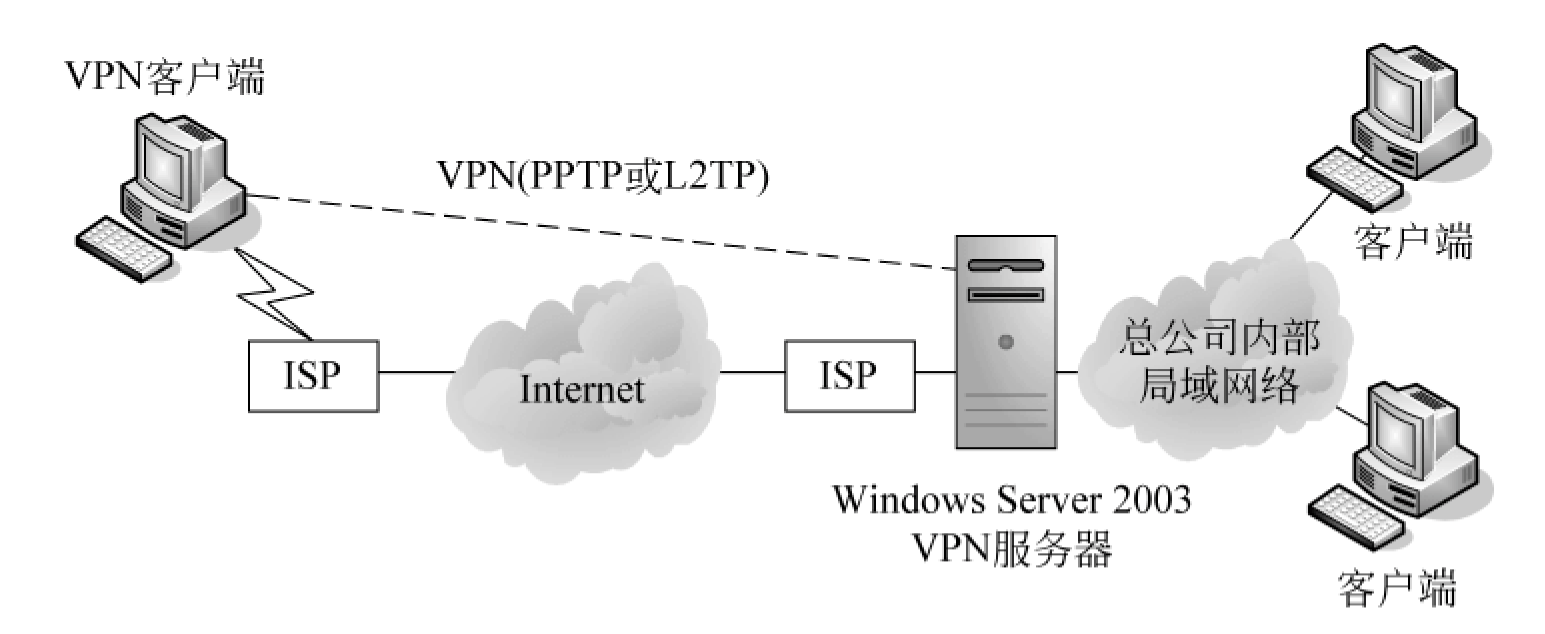


图 10-21　在客户端与总公司的网络之间建立 VPN

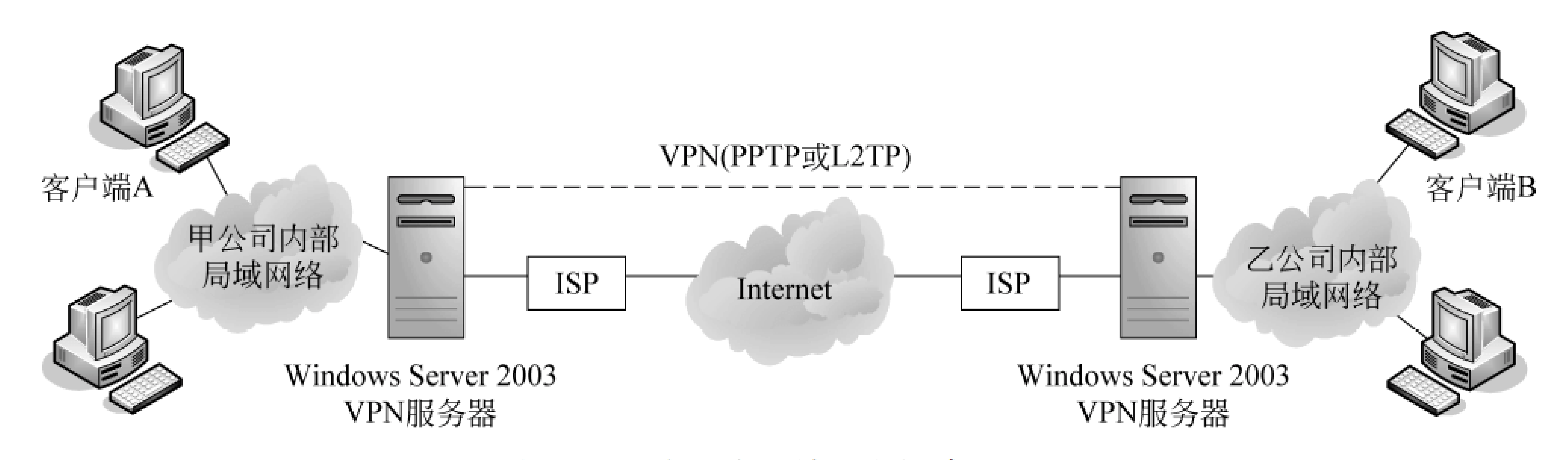


图 10-22　在两个局域网之间建立 VPN

网卡作为内部局域网接口 ETH1，另一块网卡作为连接 ADSL Modem 的 Internet 接口 ETH0。远程的 VPN 客户端也通过 ADSL Modem 接入到 Internet。

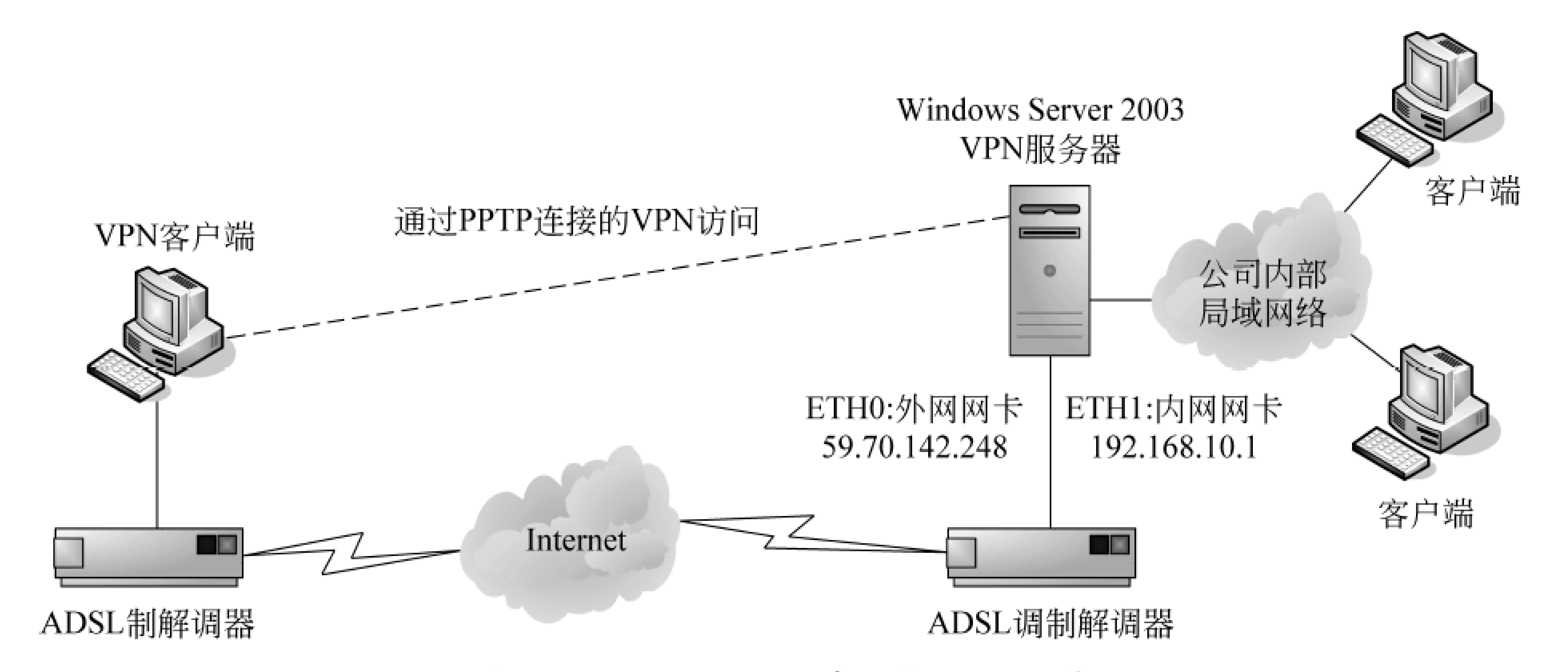


图 10-23　通过 PPTP 建立的 VPN 连接

1. VPN 服务器的安装

在 Windows Server 2003 服务器上，安装 VPN 服务的操作步骤如下。

(1) 打开“路由和远程访问”控制台，右击“SERVER01 服务器”，选择“配置并启用路由和远程访问”。在“欢迎使用路由和远程访问服务器安装向导”对话框中，单击“下一步”按钮。

（2）在图 10-24 中，选择“远程访问(拨号或 VPN)”单选按钮，单击“下一步”按钮。

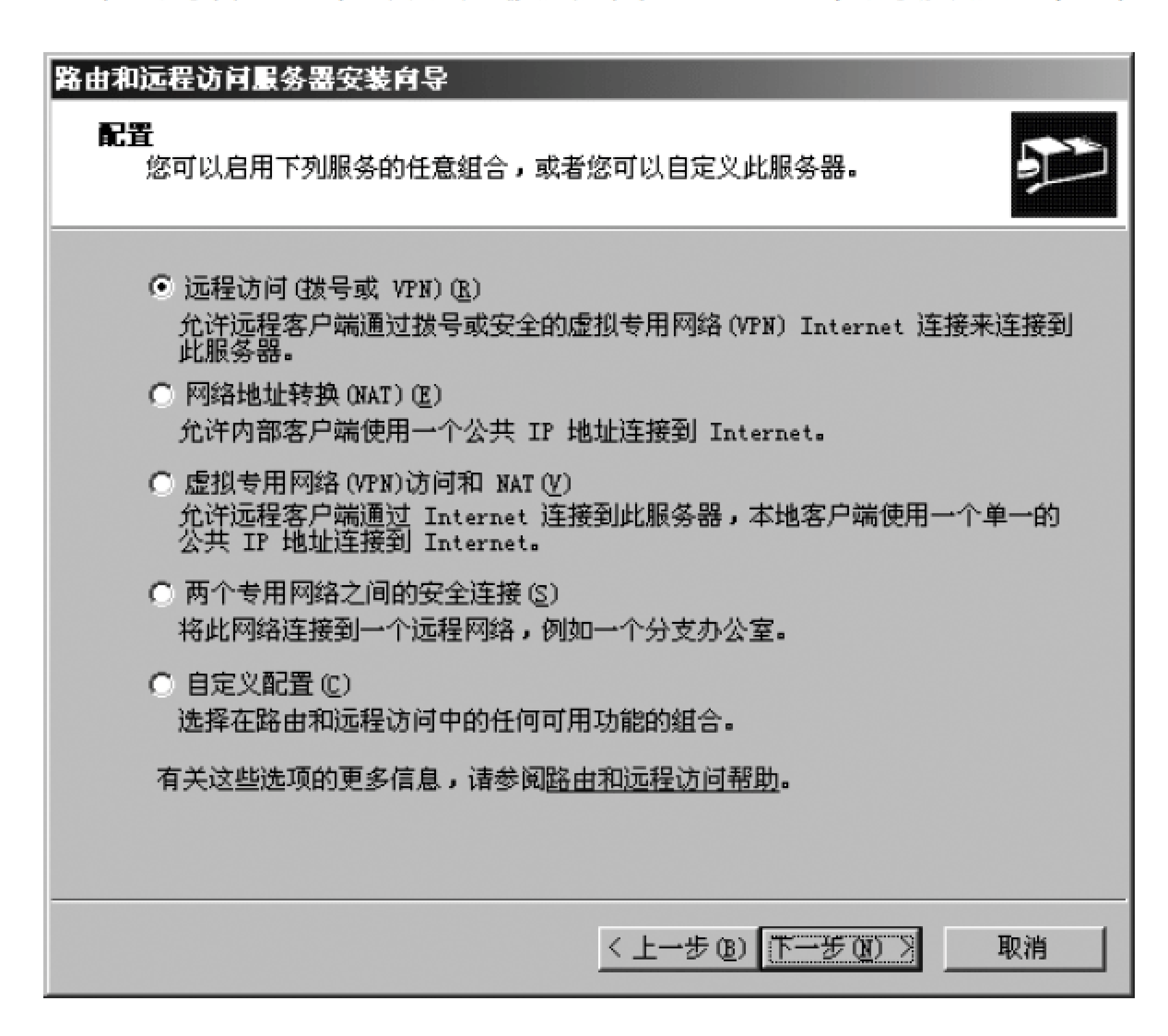


图 10-24　选择 VPN 的配置组合

（3）在图 10-25 中，配置此服务器是接受拨号连接还是 VPN 连接，在此选择 VPN 复选框，单击“下一步”按钮。

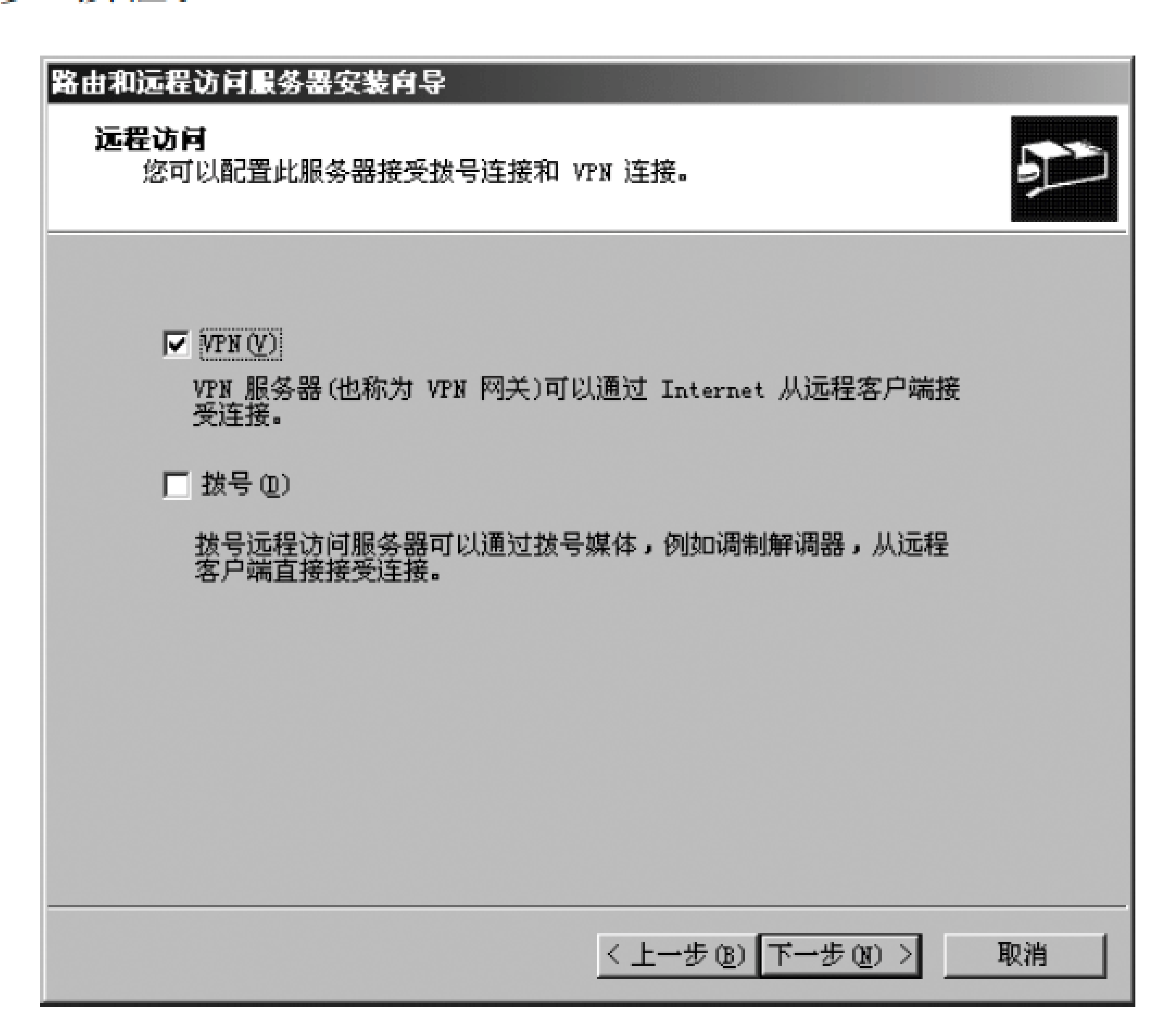


图 10-25　配置拨号连接或 VPN 连接

（4）在图 10-26 中，选择用来连接 Internet 的网络接口，在此选择外部网卡 ETH0 接口，其 IP 地址为 59.70.142.248。可以设置静态数据包筛选器保护接口，单击“下一步”按钮。

（5）在图 10-27 中，有两种选择。

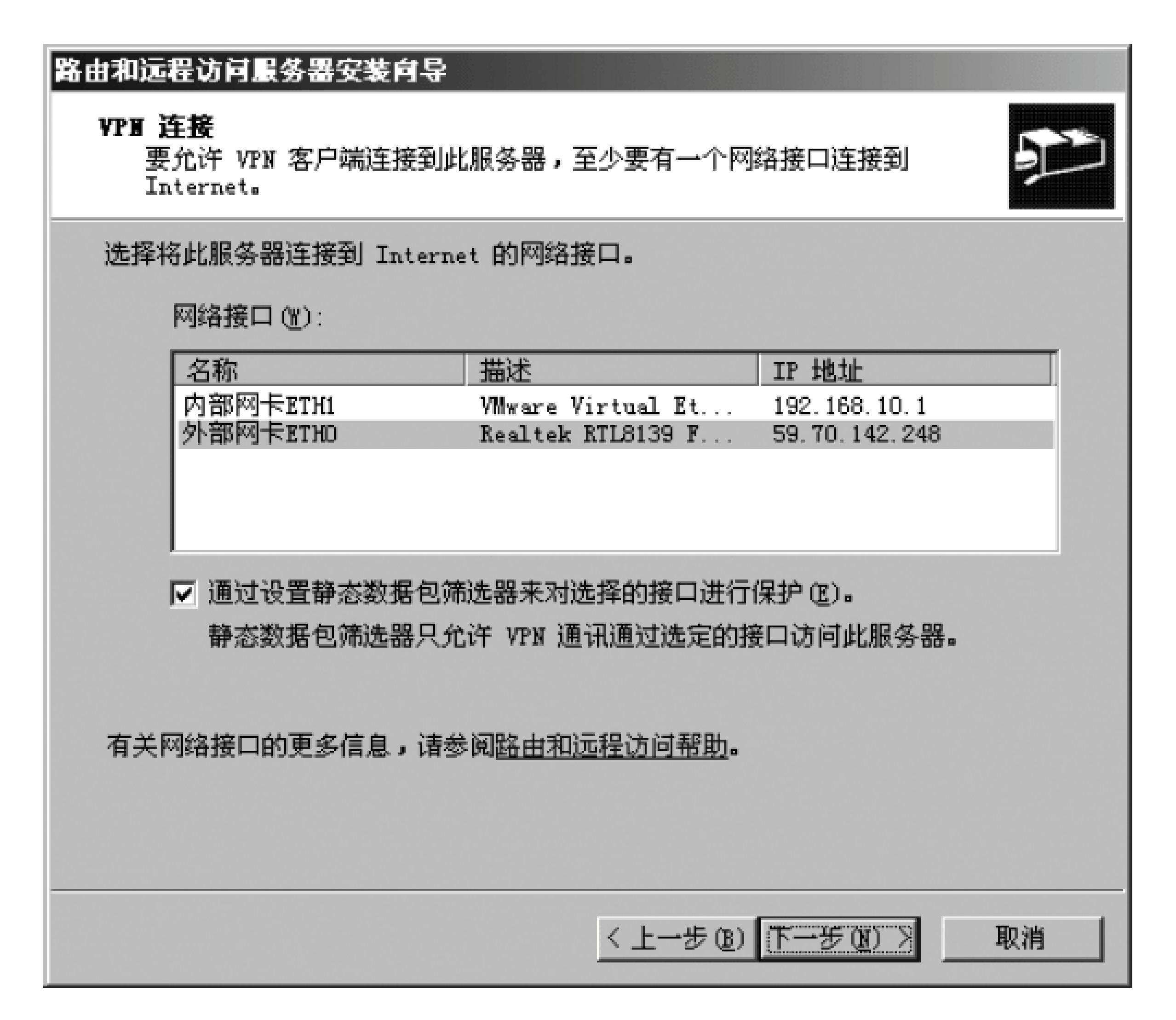


图 10-26　选择连接 Internet 的网络接口

① 自动。由 VPN 服务器向 DHCP 服务器请求 IP 地址,然后再指派给客户端。若无法从 DHCP 服务器获取 IP 地址,则自动指派 169.254.×.×的 IP 地址给客户端。

② 来自一个指定的地址范围。给 VPN 客户端分配一个指定的地址范围的 IP 地址。在此选择“来自一个指定的地址范围”单选按钮,单击“下一步”按钮。

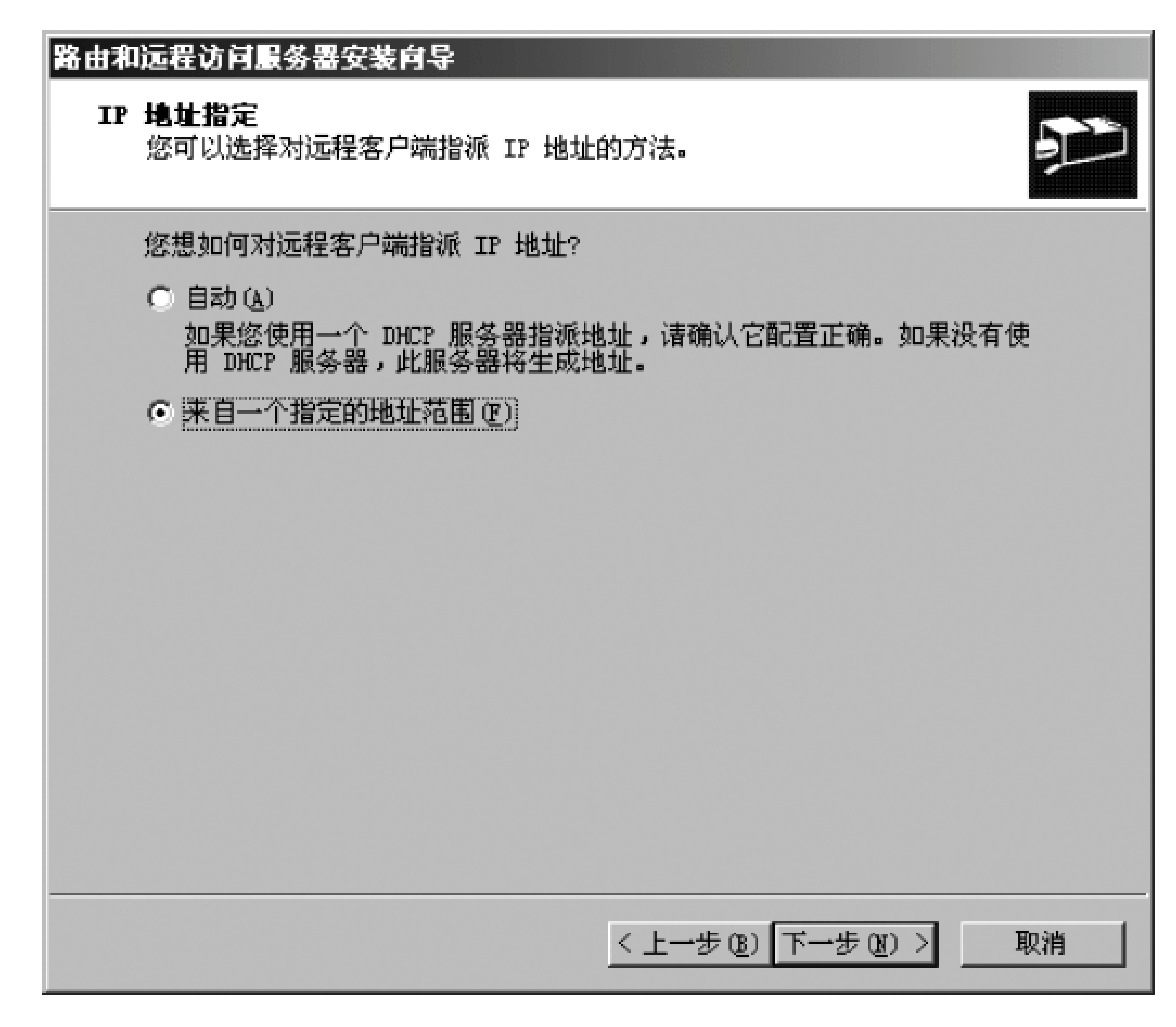


图 10-27　指定为客户端指派 IP 地址的方法

(6) 在图 10-28 中,输入起始 IP 地址和结束 IP 地址,这段地址要和 VPN 服务器的局域网接口的 IP 地址有相同的网络 ID,单击“确定”按钮。

在图 10-29 中,单击“下一步”按钮。

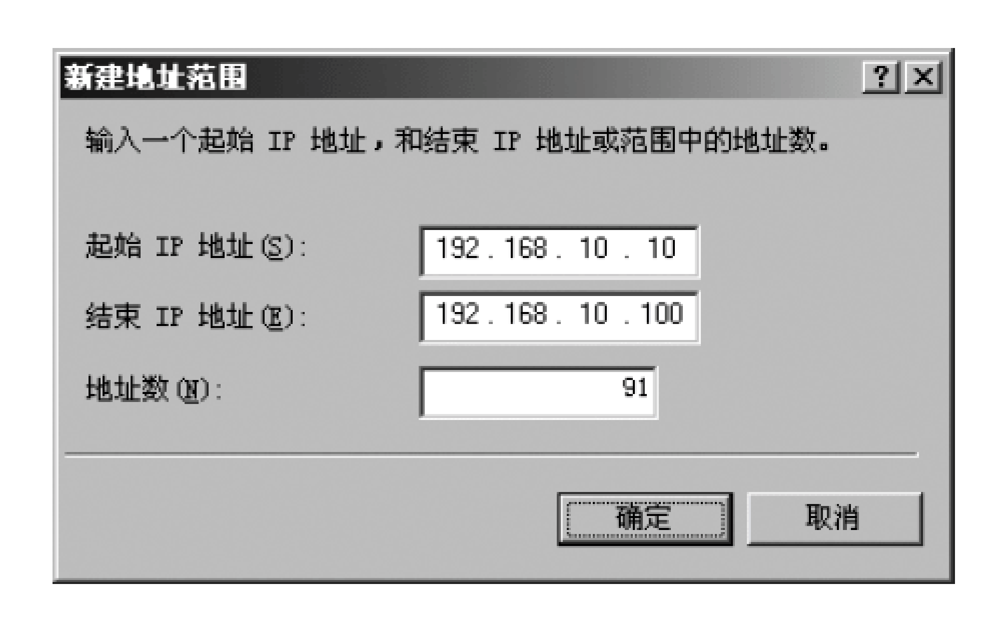


图 10-28 指定起始 IP 地址和结束 IP 地址

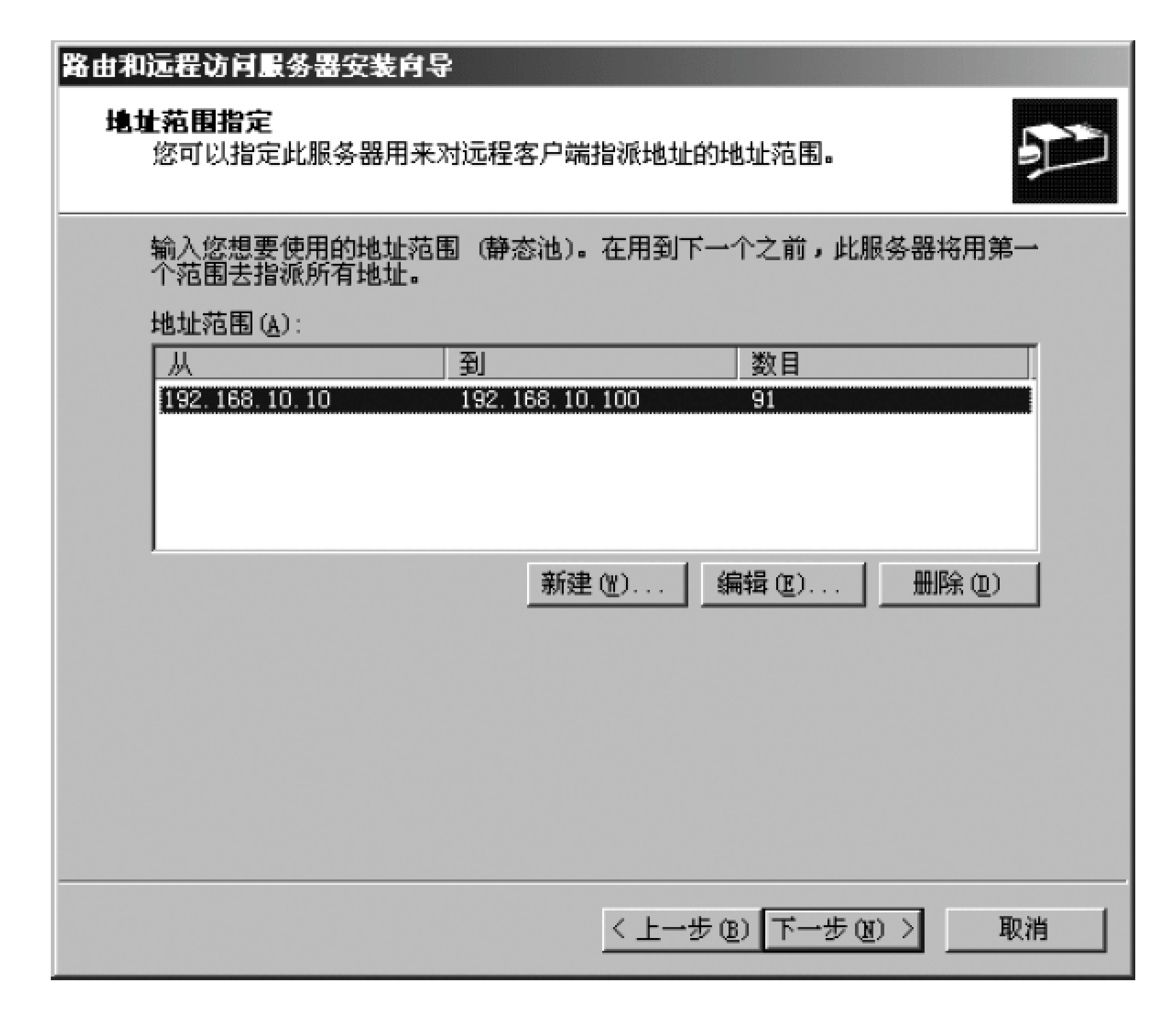


图 10-29 地址范围指定

(7) 在图 10-30 中，选择 VPN 客户端连接请求身份验证的方式。

① “否，使用路由和远程访问来对连接请求进行身份验证”单选按钮客户端请求使用路由和远程访问来对连接请求进行身份验证。

② “是，设置此服务器与 RADIUS 服务器一起工作”单选按钮网络中必须有一台 RADIUS 服务器，由 RADIUS 服务器负责 VPN 客户端身份验证请求。

在此选择“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮，单击“下一步”按钮。

(8) 在“完成路由和远程访问服务器安装向导”对话框中，单击“完成”按钮。在图 10-31 中，单击“确定”按钮，即可完成远程访问服务器的安装。

若要将远程访问客户端的 DHCP 消息转发到其他网络内的 DHCP 服务器，请通过“IP 路由选择”→“DHCP 中继代理程序”进行设置。

系统默认会自动建立 128 个 PPTP 端口与 128 个 L2TP 端口，每一个端口可供一个 VPN 客户端来连接，如图 10-32 所示。

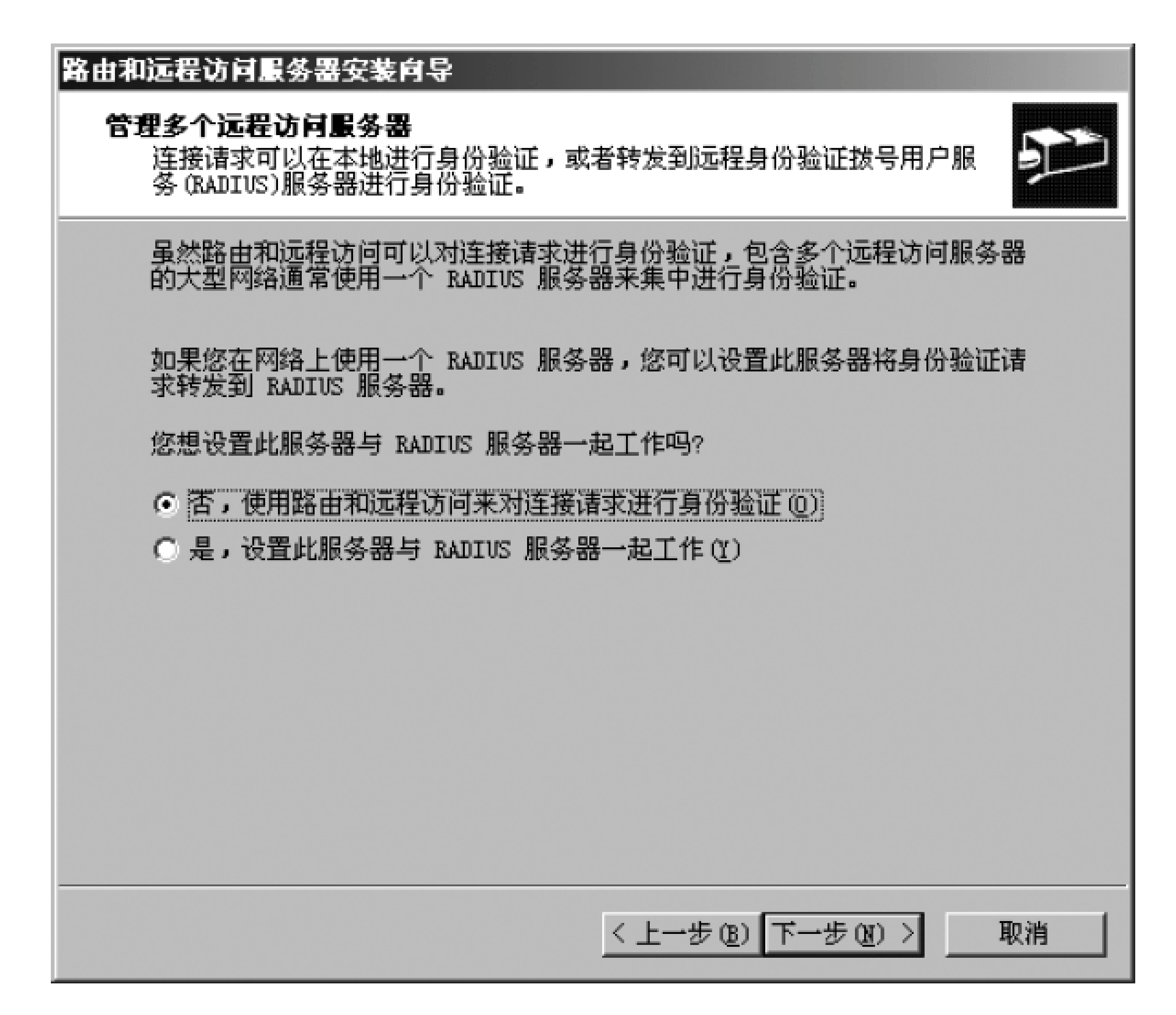


图 10-30　选择 VPN 客户端连接请求身份验证的方式

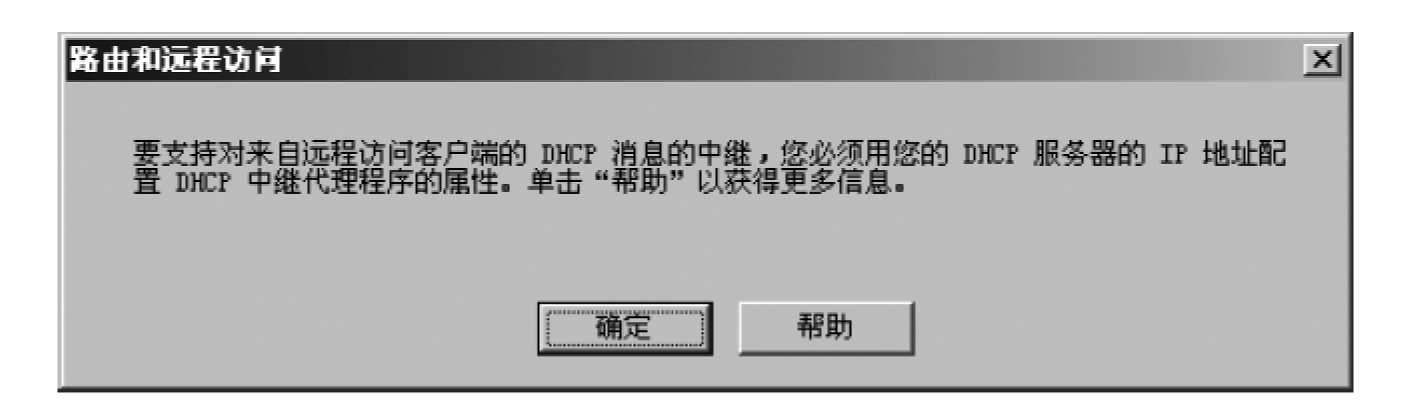


图 10-31　路由和远程访问的消息框

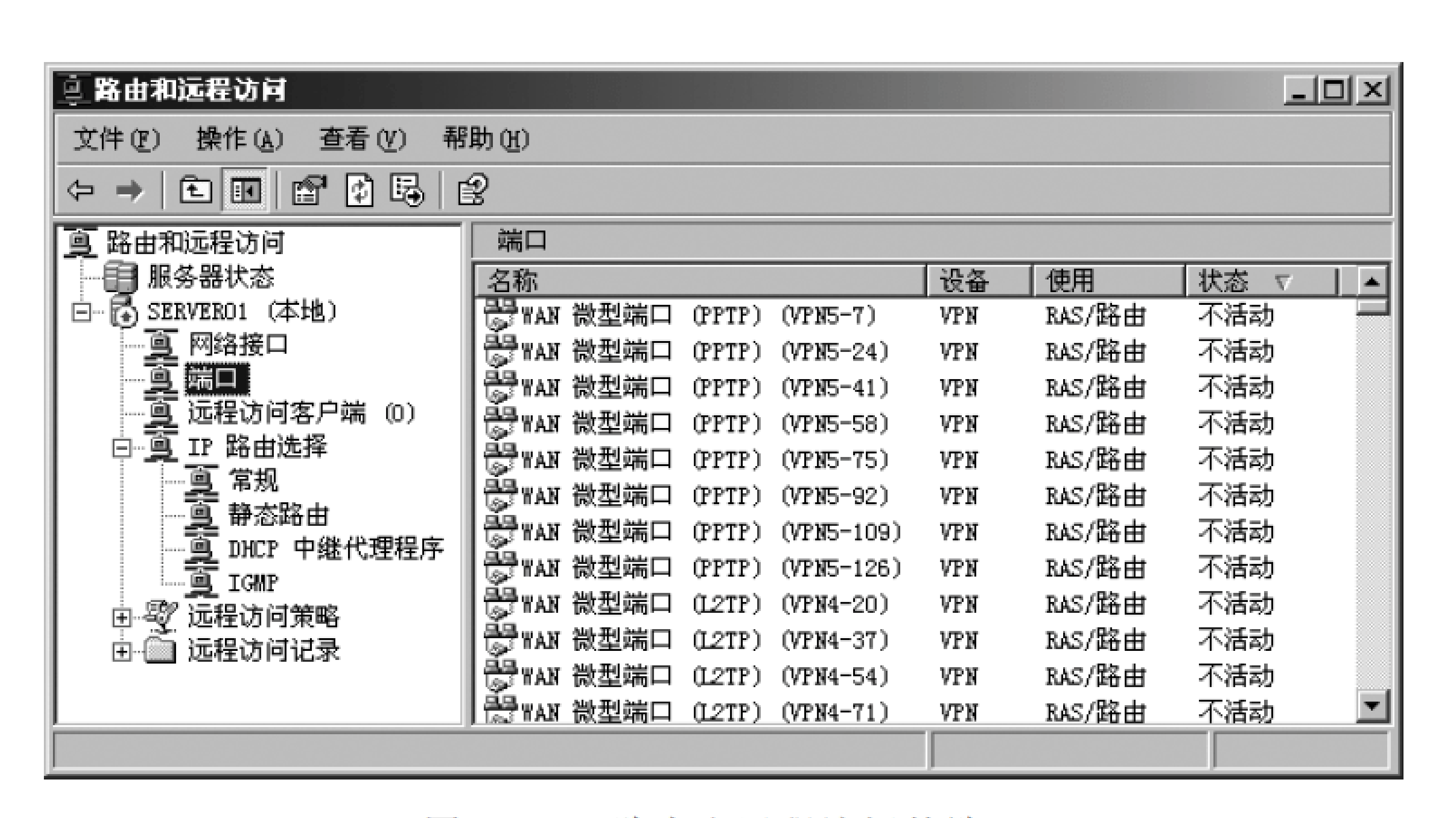


图 10-32　路由和远程访问的端口

若要更改 VPN 端口的数量，操作步骤为：右击如图 15-32 所示的"端口"→"属性"，在图 10-33 中，选择"WAN 微型端口(PPTP)"或"WAN 微型端口(L2TP)"后，单击"配置"按钮进行修改。

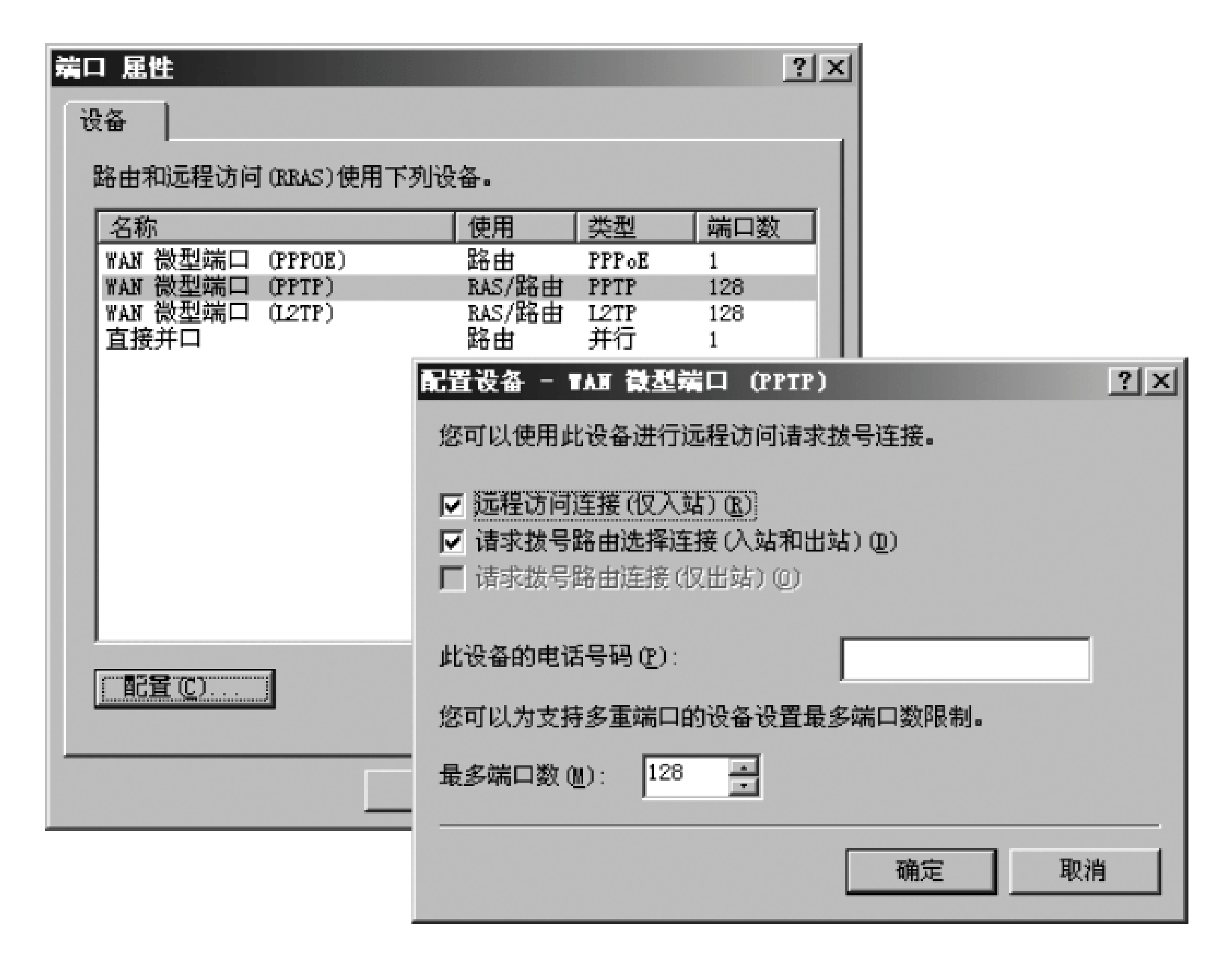


图 10-33 更改 VPN 端口的数量

2. 在 VPN 客户端建立 VPN 拨号连接

若客户端计算机已经通过 ADSL 建立了到 Internet 的连接(假设连接名为 hanet)。客户端要访问 VPN 服务器,在 VPN 服务器上必须为 VPN 客户端设置拨入权限,另外还要新建一个 VPN 客户端连接。

以 Windows Server 2003 客户端为例,建立 VPN 客户端连接的操作步骤如下。

(1) 右击"网上邻居"→"属性"→"创建一个新的连接",出现"欢迎使用新建连接向导"对话框时,单击"下一步"按钮。

(2) 在图 10-34 中,选择"连接到我的工作场所的网络"单选按钮,单击"下一步"按钮。

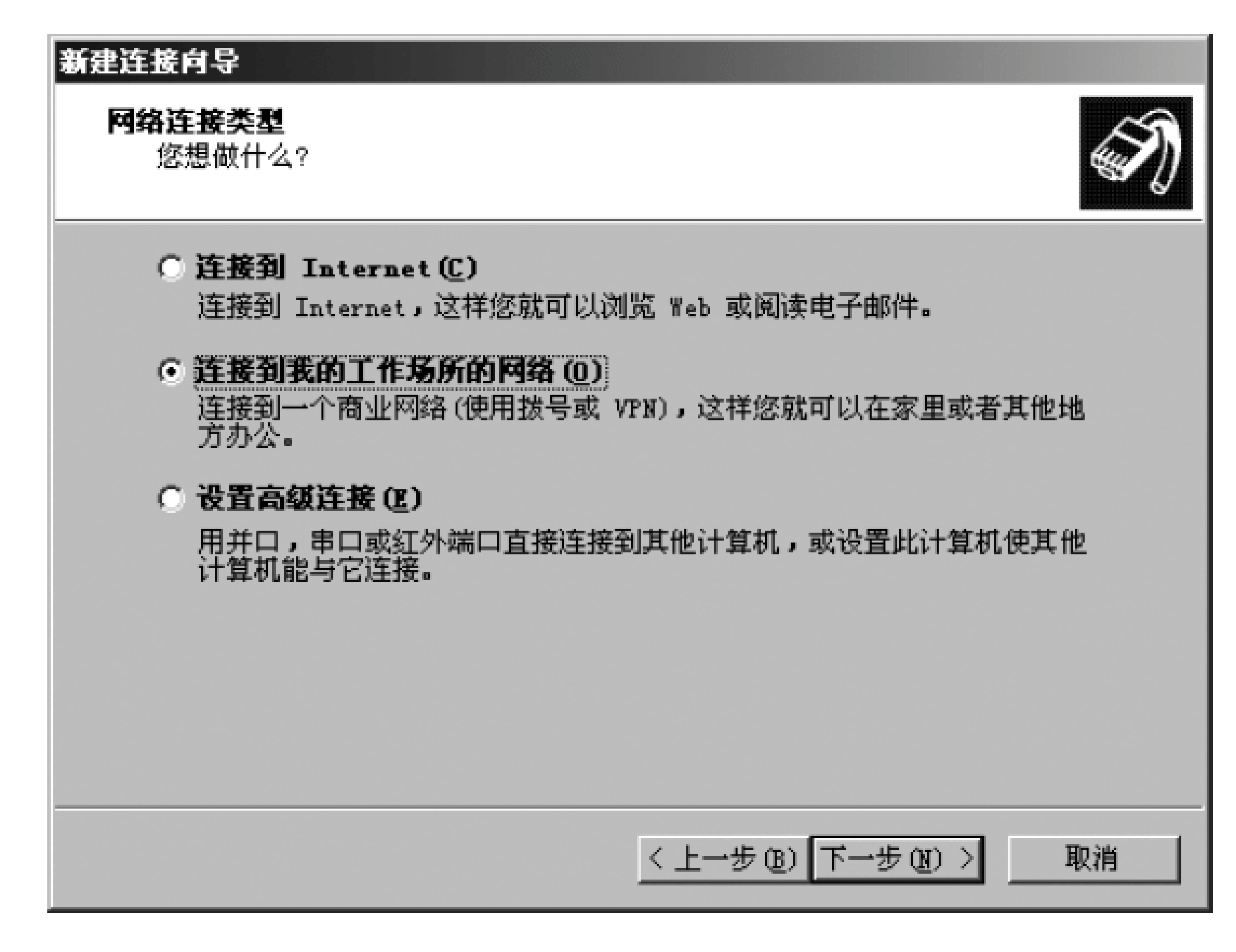


图 10-34 网络连接类型

(3)在图10-35中,选择“虚拟专用网络连接”单选按钮,单击“下一步”按钮。

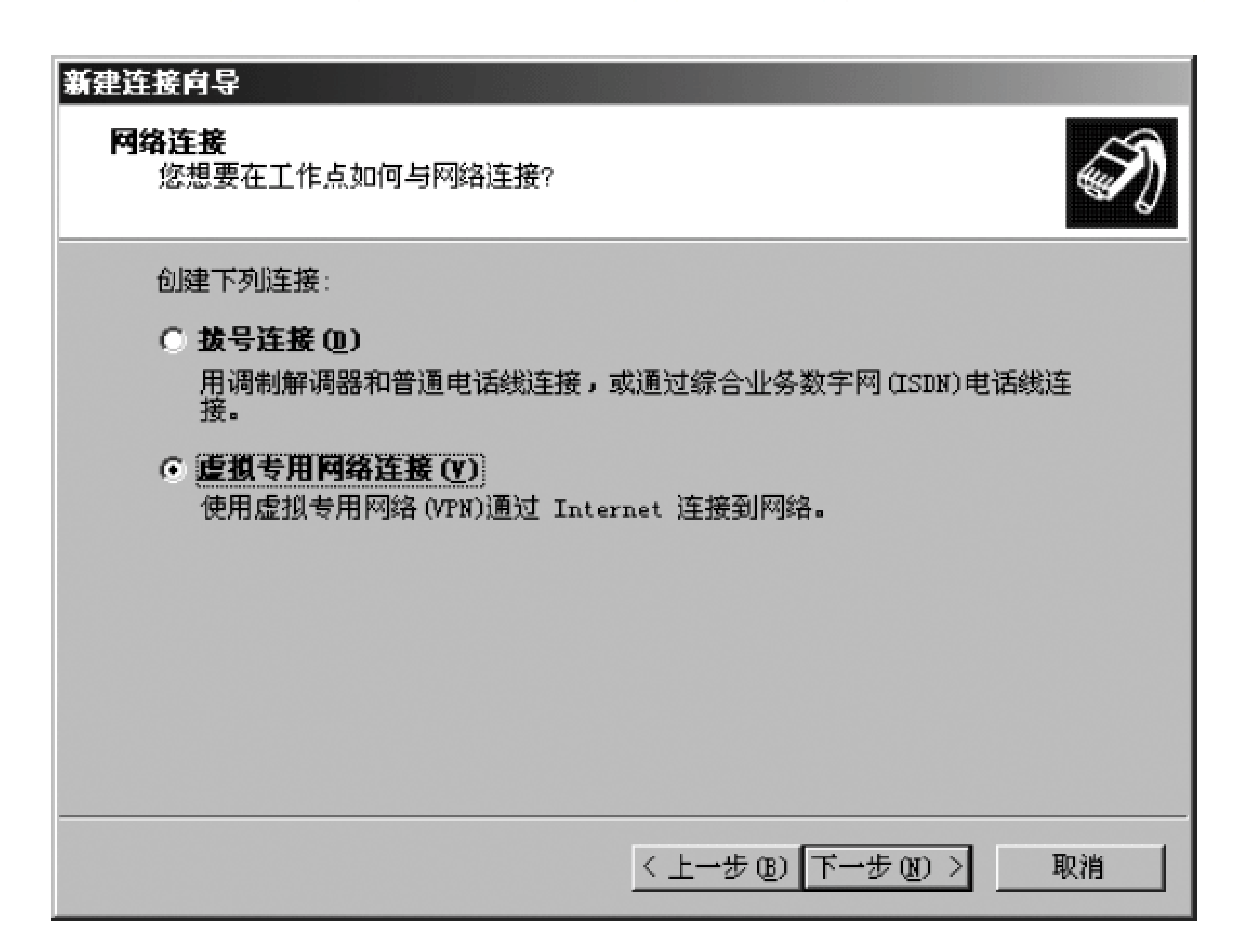


图10-35　指定建立网络连接的方式

(4)在图10-36中,输入公司名,例如总公司信息中心,单击“下一步”按钮。

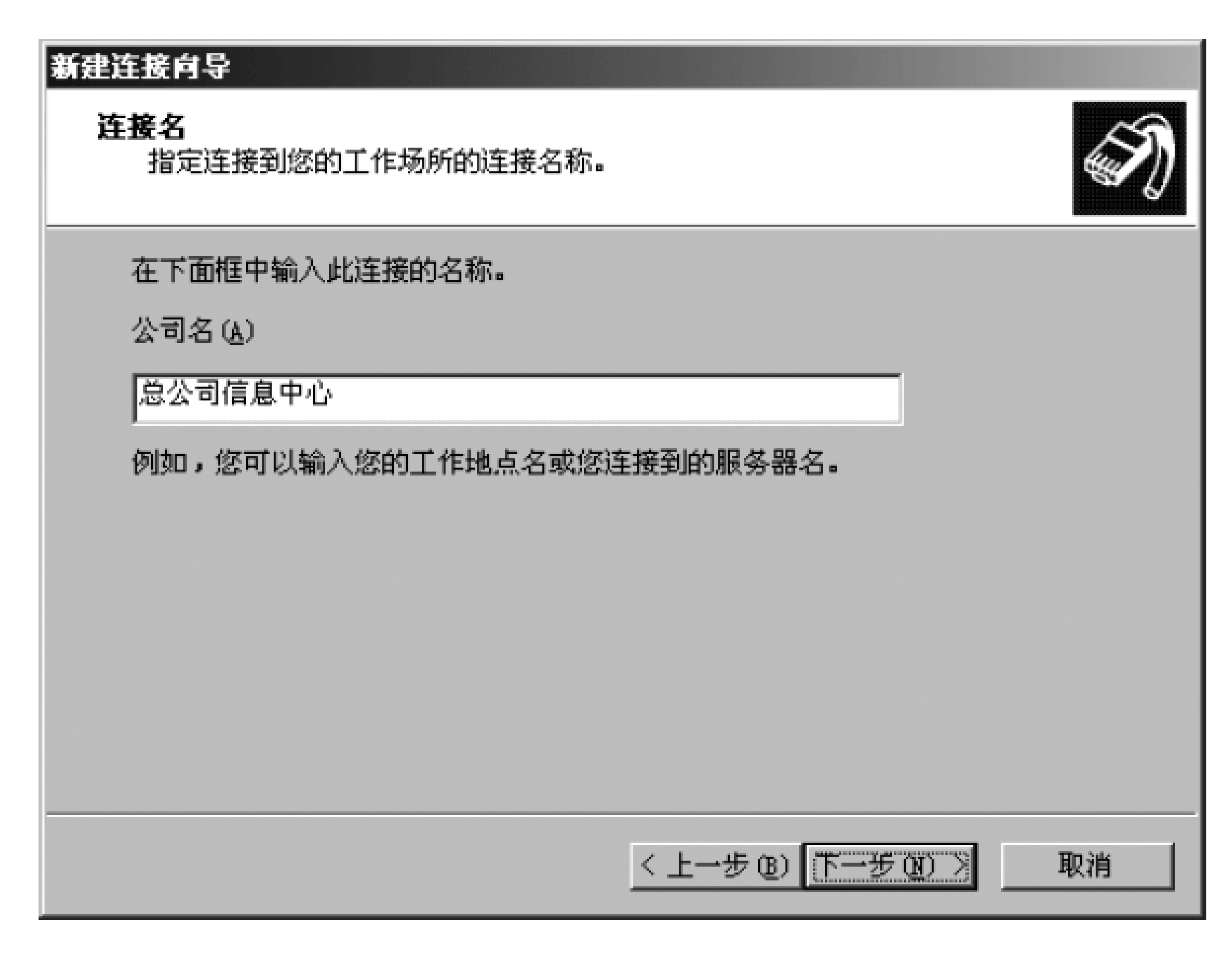


图10-36　指定连接名称

(5)在图10-37中,有两种选择,在此选择“自动拨此初始连接”单选按钮,并选择客户端利用ADSL调制解调器与ISP建立的连接名称,单击“下一步”按钮。

提示:如果使用的是一直在线的宽带网络而不是通过ADSL调制解调器接入Internet,在建立VPN客户端连接时,则不会出现此步骤,其他步骤相同。

(6)在图10-38中,输入VPN服务器的主机名或IP地址,在此输入IP地址59.70.142.248,单击“下一步”按钮。

(7)在图10-39中,设置此连接是供任何人使用还是只有建立此连接的用户才可以使用。在此选择“任何人使用”单选按钮,单击“下一步”按钮。

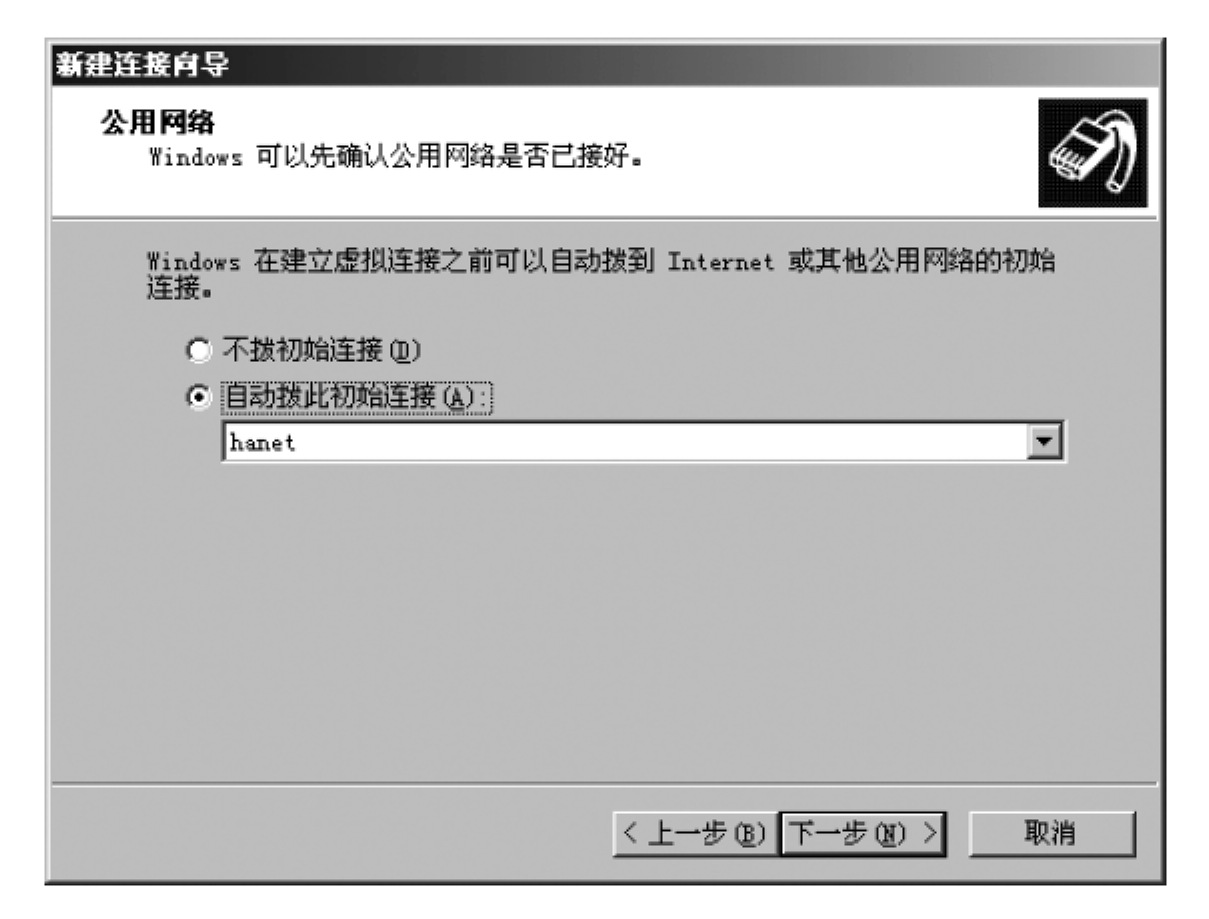


图 10-37 指定是否拨初始连接

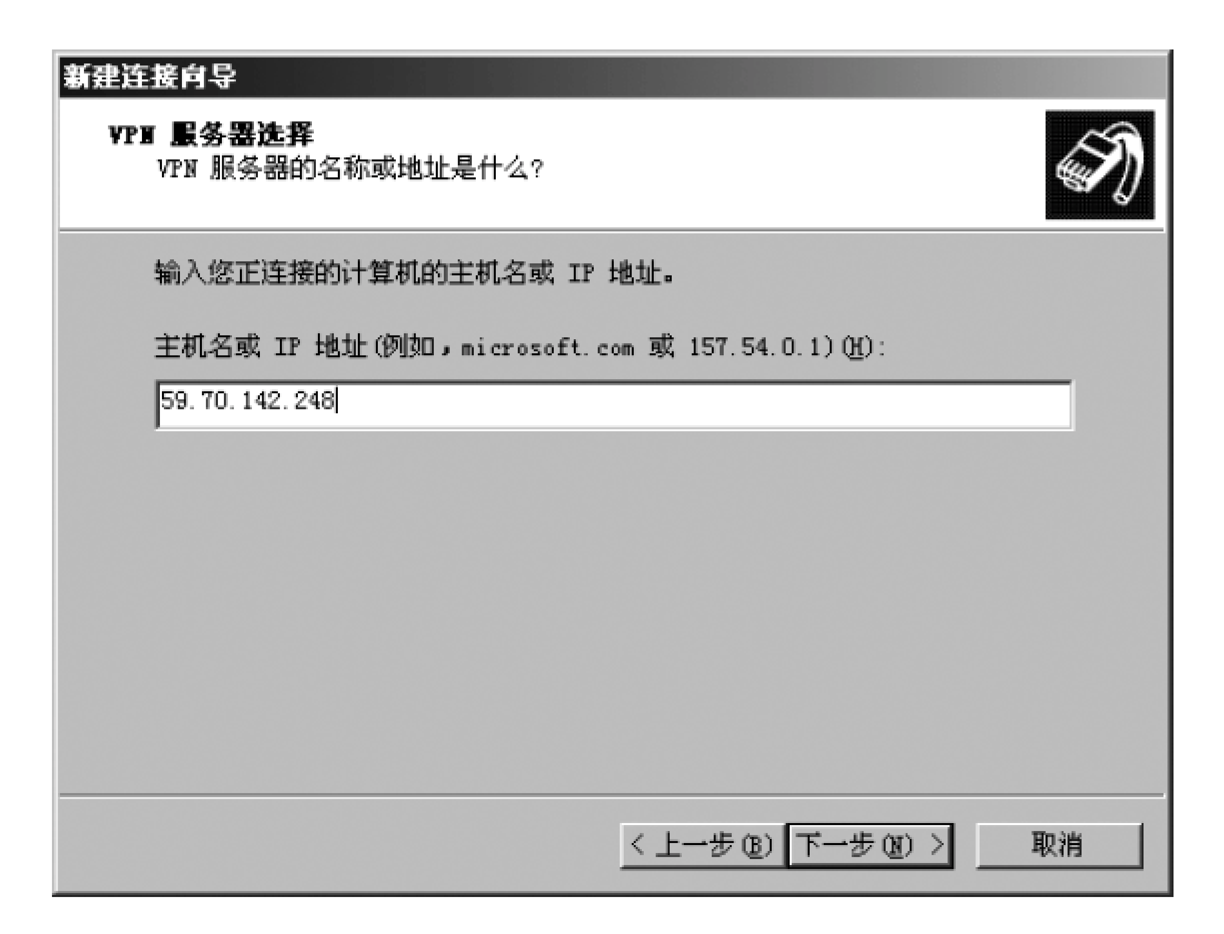


图 10-38 输入 VPN 服务器的主机名或 IP 地址

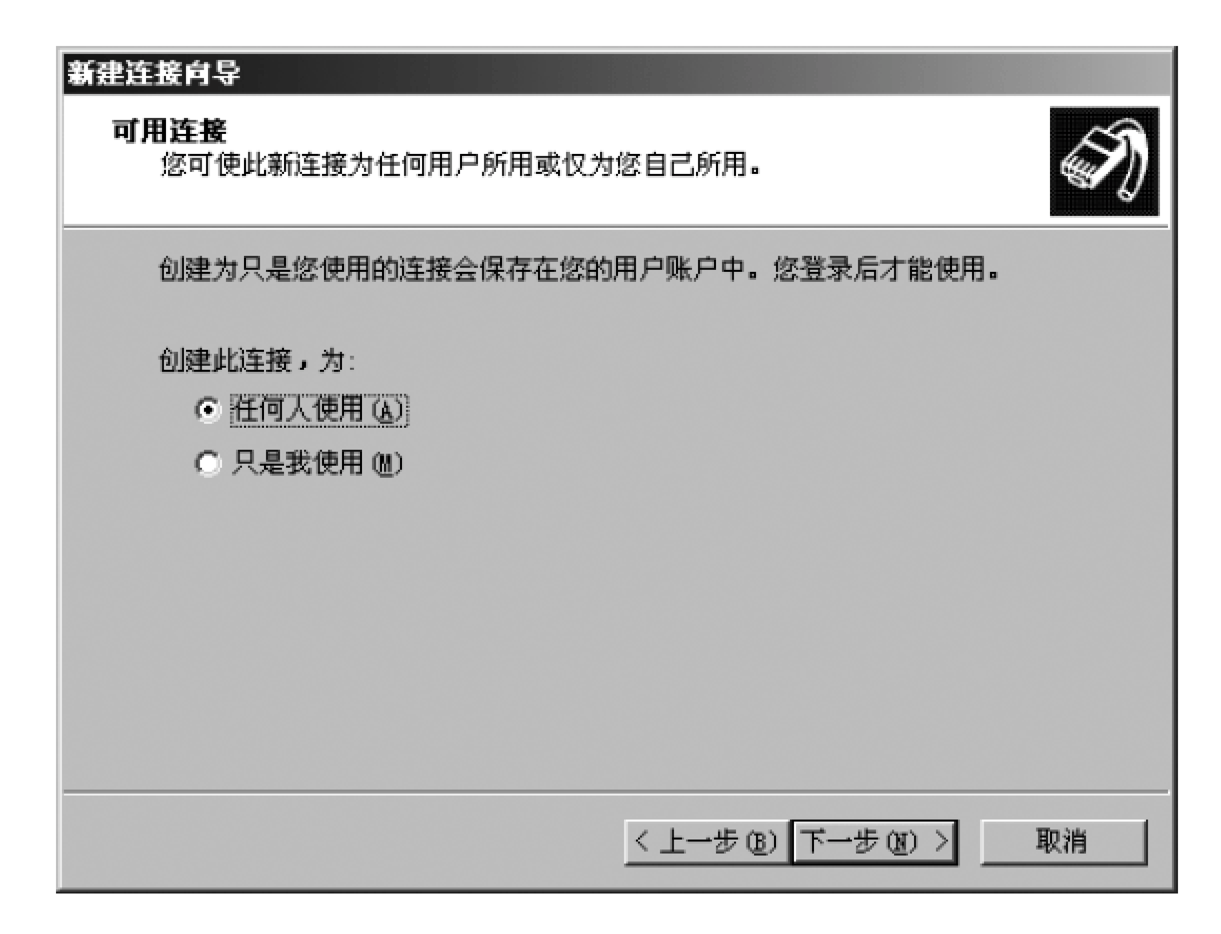


图 10-39 可用连接

（8）在“完成新建连接向导”对话框中，单击“完成”按钮即可完成 VPN 客户端的配置。

在确保客户端已经通过 ADSL 连接到 Internet 之后，用户可以通过右击“网上邻居”→“属性”→双击创建的虚拟专用网络连接，打开“登录”对话框，输入用来连接远程访问服务器的用户名与密码后，单击“连接”即可连接到 VPN 服务器。

在 VPN 服务器上可以检查 VPN 服务器的使用情况，如图 10-40 所示，有个 PPTP 的 VPN 连接状态为“活动”，说明已经有 VPN 客户端通过 PPTP 连接到 VPN 服务器。



图 10-40　活动的 VPN 连接

第 11 章　路由与 NAT

学习目标

学习完本章后，了解 Windows Server 2003 路由、网络地址转换（Network Address Translation，NAT）的工作原理，掌握 Windows Server 2003 路由、NAT 及数据包筛选器的配置方法，并掌握静态路由和 RIP 动态路由协议的应用。

11.1　路由器的工作原理

路由器是一种连接多个网络或网段的设备，并在这些网络或网段之间转发数据包。路由器可以是专用的硬件路由器，例如 Cisco、华为路由器，也可以是启用了“路由和远程访问”服务的 Windows Server 2003 软路由器。

在图 11-1 所示的网络中，甲、乙、丙 3 个网络利用两台 Windows Server 2003 软路由器来连接，以 3 个不同的私有 IP 地址段来代表 3 个不同的网络。假设甲网络内的客户端 A 要与乙网络内的客户端 E 通信，客户端 A 会将数据传送到路由器 A，然后路由器 A 会将其转发给路由器 B，最后再由路由器 B 负责将其传送给乙网络内的客户端 E。

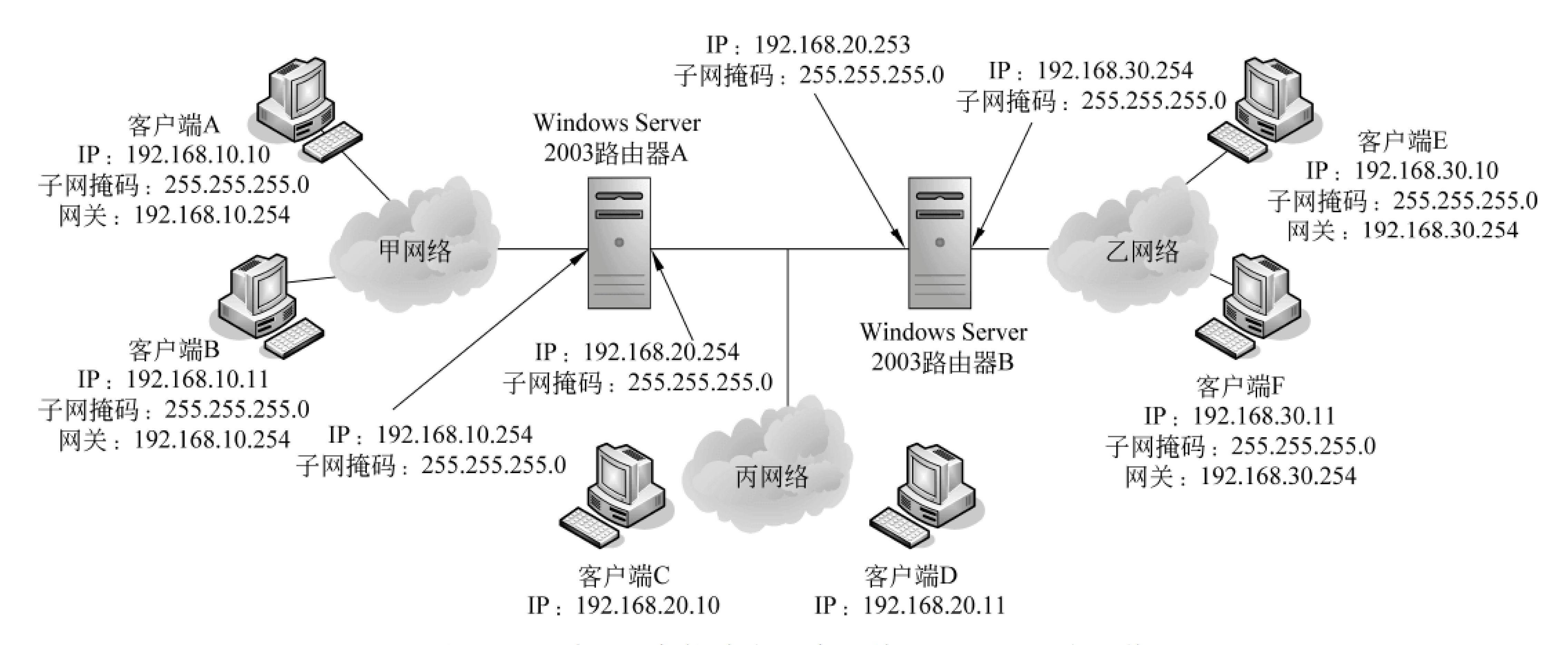


图 11-1　利用两台软路由器来连接甲、乙、丙 3 个网络

根据数据包目标地址的不同，发送主机必须决定是将数据发送给目标主机还是转发给路由器。当发送主机转发数据时，就会使用主机路由。当路由器接收到需要转发的报文时，就会使用路由器的路由，如图 11-2 所示。

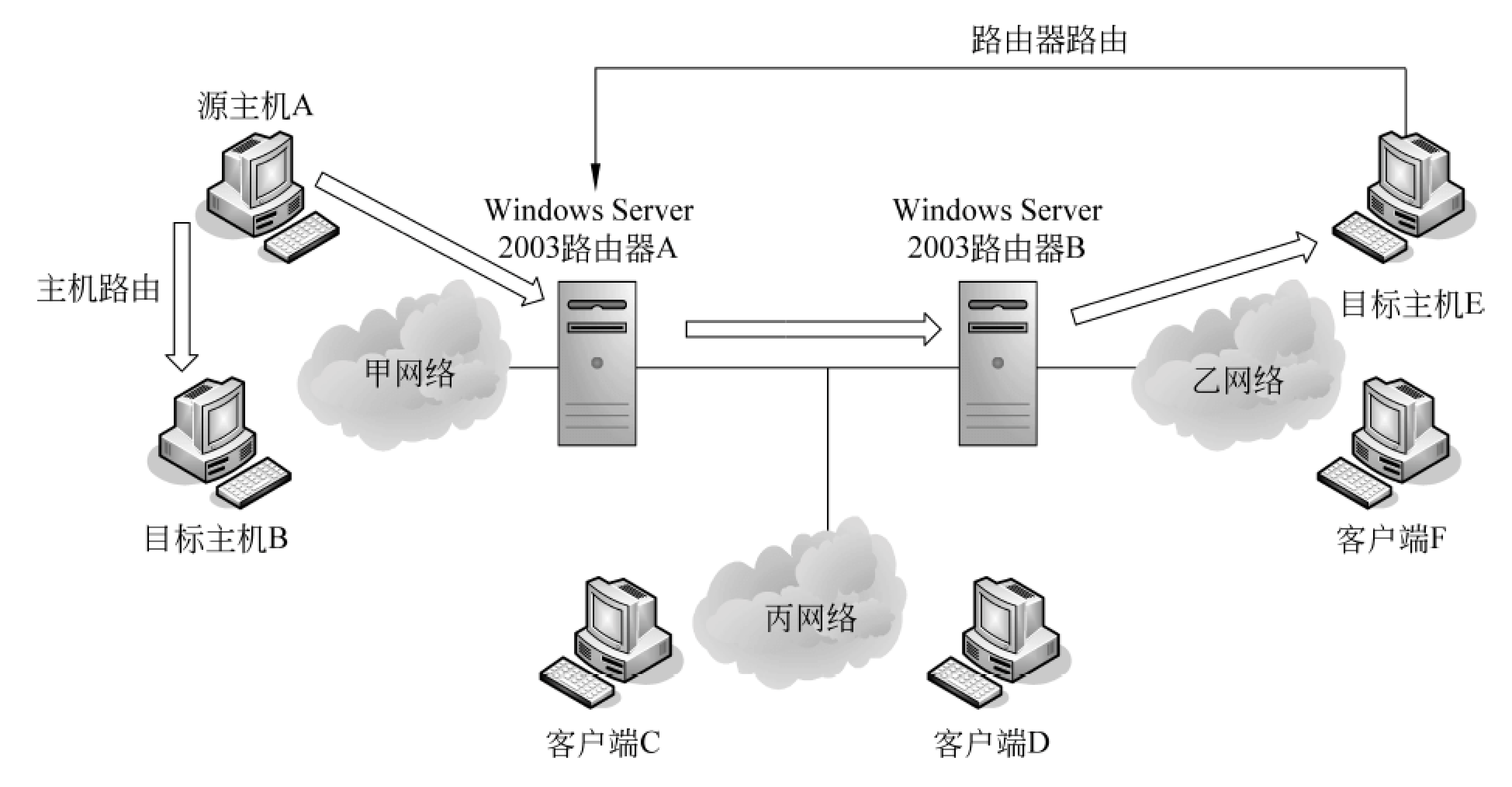


图 11-2　主机路由和路由器路由

11.1.1　主机路由表

在安装了可路由协议(例如 TCP/IP)的计算机(例如源主机 A)上,在命令提示符下,执行 route print 命令,就可以得到该主机的路由表,如图 11-3 所示。

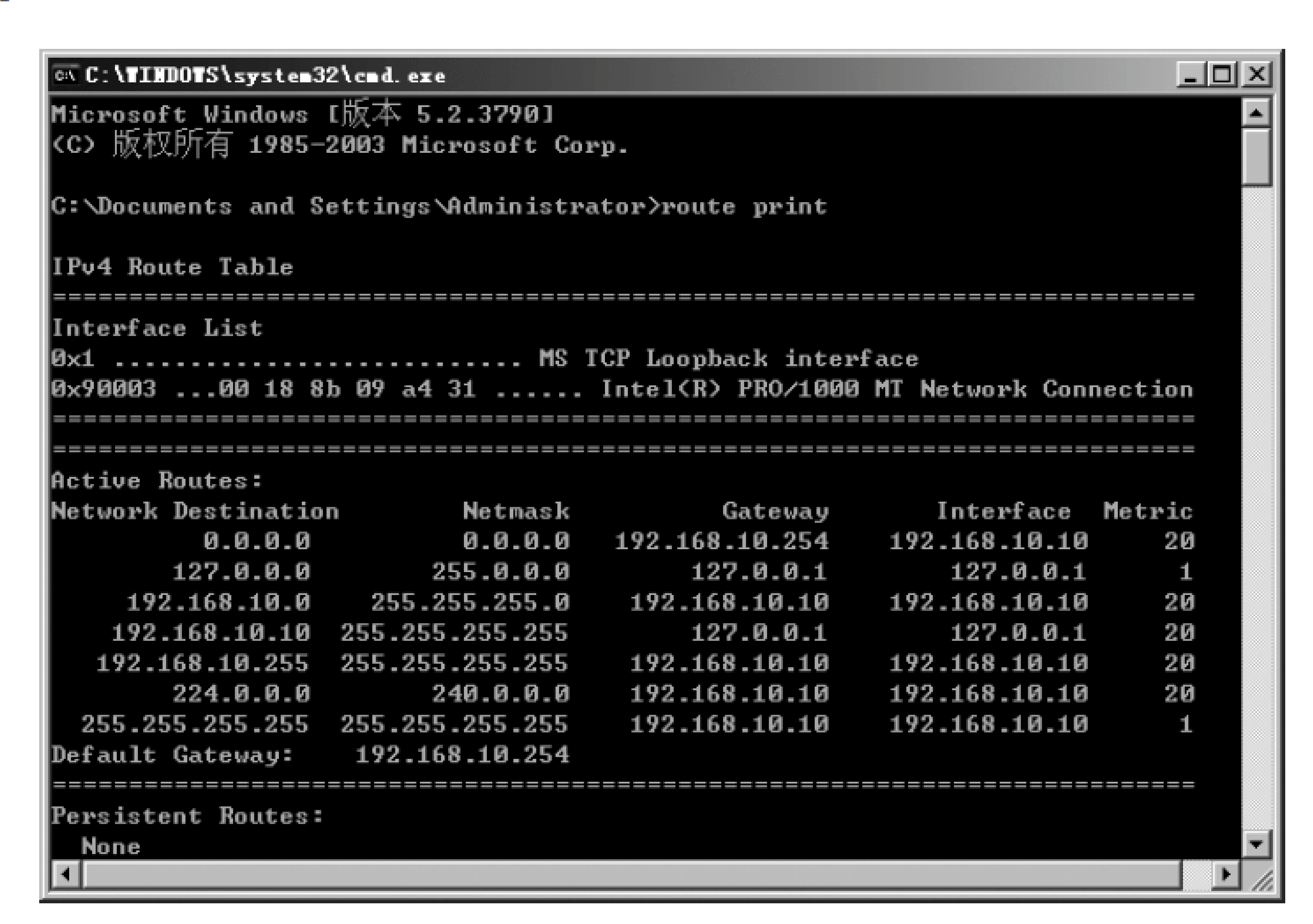


图 11-3　主机的路由表

其中:

(1) Network Destination 即目标网络地址,可以是一个网络或是一个 IP 地址。

(2) Netmask 即网络掩码或子网掩码。

(3) Gateway 即网关,如果目标计算机的 IP 地址与 Netmask 执行逻辑与(AND)运

算后的结果，等于 Network Destination 处的值，就会将数据转发给 Gateway 处理。如果 Gateway 处的 IP 地址又等于源主机 A 自己的 IP 地址，就会将数据直接传送给目标计算机，这时说明源主机和目标主机在同一个网络(具有相同的网络 ID)。例如，源主机 A 和目标主机 B 通信时就是这样。

(4) Interface 即接口，表示数据是从计算机 A 的这个 IP 地址转发。

(5) Metric 即度量值，表示通过此路由来转发数据的成本，Metric 值越小，路由越好。通常使用链路的带宽、延迟、负载、可靠性、从源到目标数据包要经过的跳数(hop)等因素来衡量路由的好坏。

以下解释图 16-3 中的每一行信息的含义。

第一行代表“默认路由”，当计算机 A 要发送数据包时，如果在其路由表内找不到其他可以用来转发此数据包的路由，该数据包就会通过默认路由来转发，也就是说数据包将从 IP 地址为 192.168.10.10 的 Interface 送出，然后传送给 IP 地址为 192.168.10.254 的 Gateway。

第二行代表“环回路由”，当计算机 A 要传送数据包到类似于 127.x.y.z 的 IP 地址时，这些数据包都将从 IP 地址为 127.0.0.1 的 Interface 送出，然后传送到 IP 地址为 127.0.0.1 的 Gateway。127.0.0.1 是计算机的回环地址。

第三行代表“直连路由”，当计算机 A 要传送数据包给 192.168.10.0 这个网络的计算机时，该数据包都将从 IP 地址为 192.168.10.10 的 Interface 送出，而在 Gateway 处的 IP 地址 192.168.10.10 为计算机 A 自己的 IP 地址，表示将数据包直接传送给目标地址。

第四行代表“主机路由”，当计算机 A 要传送数据包到 192.168.10.10(计算机 A 自己)时，该数据包将从 IP 地址为 127.0.0.1 的 Interface 送出，然后传送到 IP 地址为 127.0.0.1 的 Gateway。127.0.0.1 是计算机的回环地址。

第五行代表“子网广播路由”，当计算机 A 要传送数据包给 192.168.10.255 时，该数据包将从 IP 地址为 192.168.10.10 的 Interface 送出，而在 Gateway 处的 IP 地址 192.168.10.10 为计算机 A 自己的 IP 地址，表示将数据包将直接传送给目标地址。

第六行代表“多播路由”，当计算机 A 要发送多播数据包时，该数据包将通过 IP 地址为 192.168.10.10 的 Interface 送出，而在 Gateway 处的 IP 地址 192.168.10.10 为计算机 A 自己的 IP 地址，表示数据包将直接传送给目标地址。

第七行代表“有限的广播路由”，当计算机 A 要传送广播数据包到 255.255.255.255 时，该数据包将通过 IP 地址为 192.168.10.10 的 Interface 送出，而在 Gateway 处的 IP 地址 192.168.10.10 为计算机 A 自己的 IP 地址，表示数据包将直接传送给目的地址。

11.1.2 路由器路由表

在路由器 A 的命令提示符下，执行 route print 命令可以显示路由器 A 的路由表，如图 11-4 所示。因该路由表与主机路由表类似，在此仅对度量(Metric)值做部分说明。

路由器有多个接口，因此会有多个默认路由。如果路由器通过默认路由来传送数据包，路由器会选择子网掩码长度最长(即二进制位为 1 的数目最多)的路由作为最佳路由。

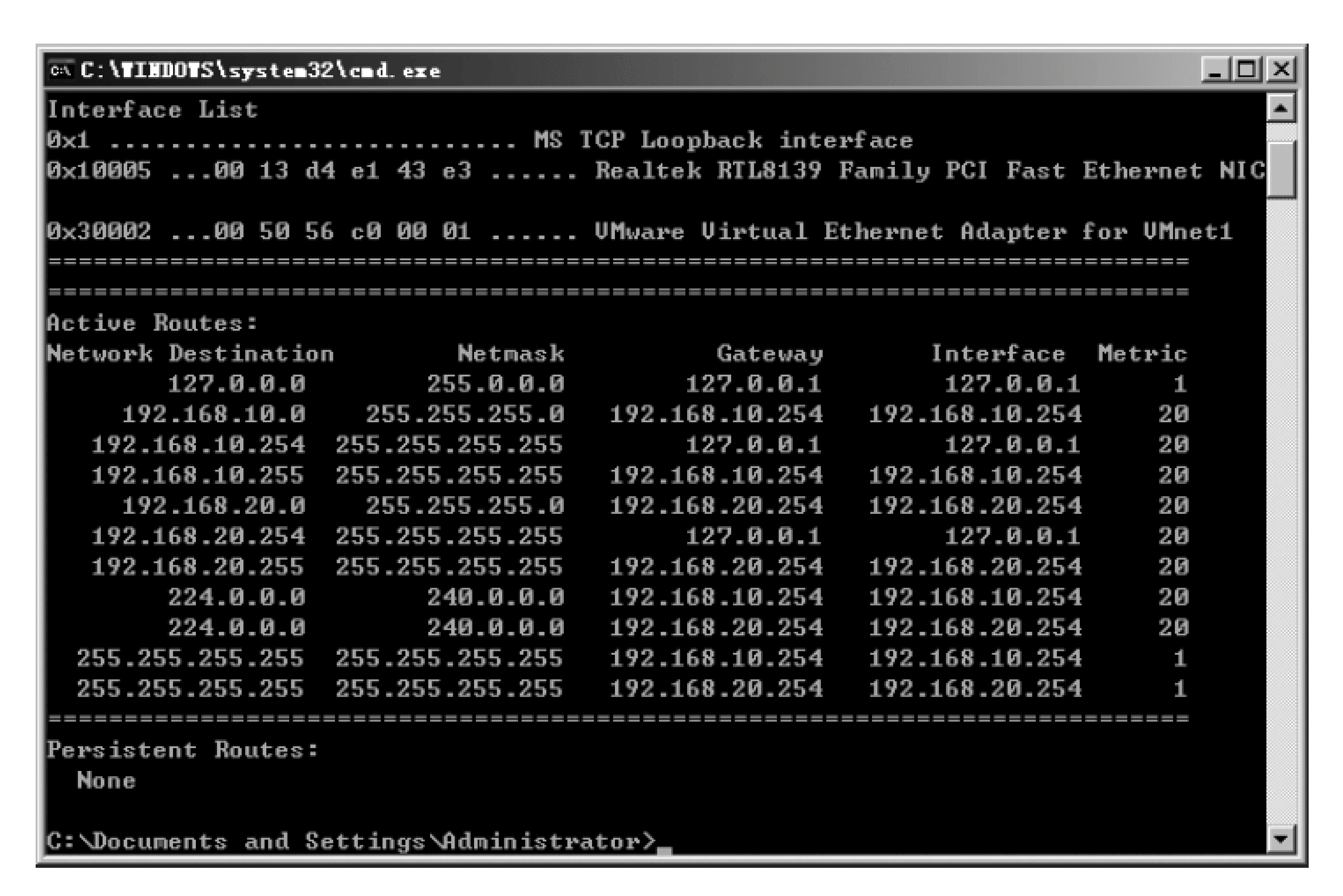


图 11-4　路由器 A 的路由表

若默认路由的子网掩码都是 0.0.0.0，此时要由路由表中的 Metric 值来决定最佳路径。

Metric 即度量值，表示通过此路由来转发数据的成本，Metric 值越小，路由越好。通常使用链路的带宽、延迟、负载、可靠性、从源到目标数据包要经过的跳数(hop)等因素来衡量路由的好坏。若使用 RIP 路由协议，Metric 的值就取决于从源到达目的需要经过的跳数。如果源和目标在同一网络内，则算 1 跳，之后每经过一个路由器加 1 跳。路由器会优先使用成本最低的路由，也就是 Metric 值最小的路由，如果 Metric 值相同，则路由器会从中随机挑选一个路由。

默认情况下，每一个网络接口都会依据接口的连接速度自动计算 Metric 值，也可以手动设置接口的 Metric 值。要手动设置接口的 Metric 值，操作步骤(以路由器 A 为例)如下。

单击“开始”→“控制面板”→“网络连接”→“属性”→“高级”，取消选中“自动跃点计数”复选框，并在“接口跃点数”处输入 Metric 值，如图 11-5 所示。

图 11-5　手动设置接口的 Metric 值

当一个网络接口设置了多个网关时，系统会优先选用度量值最低的网关。若未单独设置每一个网关的度量，则所有网关的度量值都会继承网络接口的度量设置值。

11.2　配置 Windows 路由

甲、乙、丙 3 个网络利用两台 Windows Server 2003 路由器来连接，以 3 个不同的私有 IP 地址段来代表 3 个不同的网络，如图 11-6 所示。

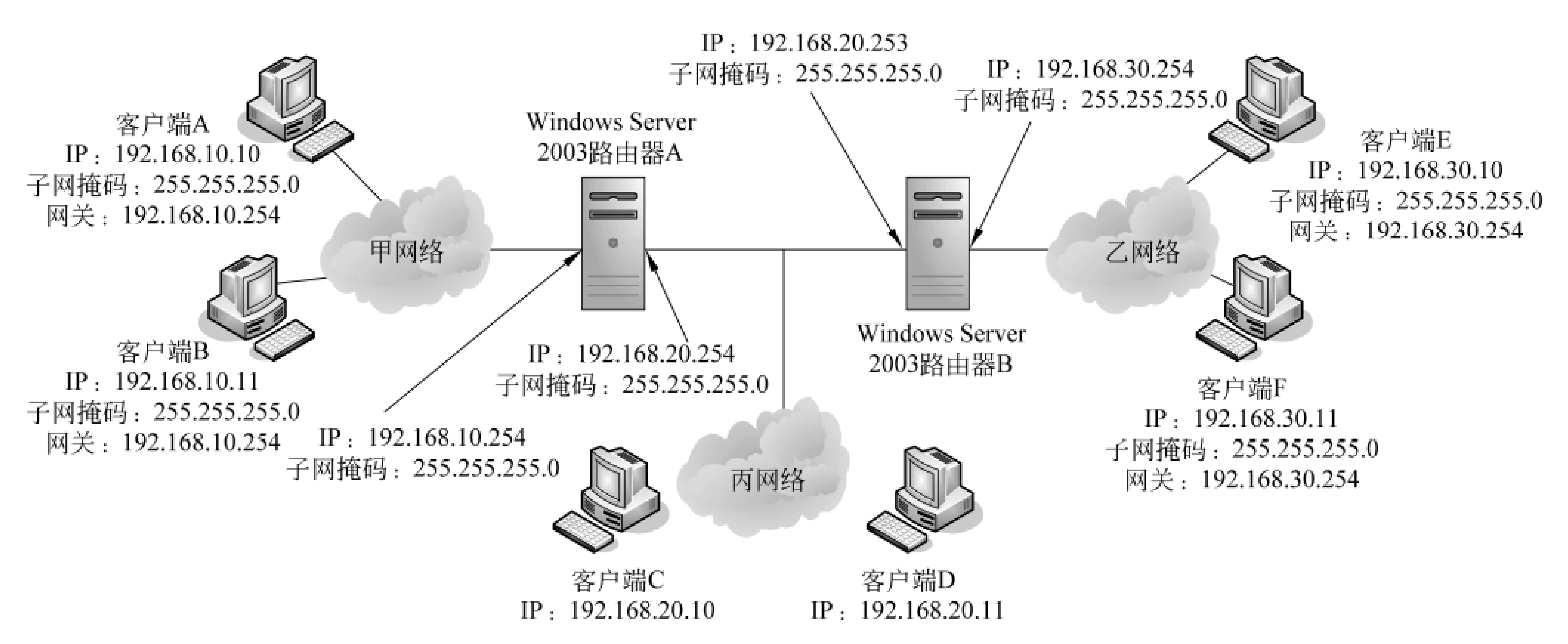


图 11-6　通过路由器 A、B 连接甲、乙、丙 3 个网络

11.2.1　启动路由器

通过启用“路由和远程访问”服务来启动路由器。

安装、配置 Windows 路由器的操作步骤如下。

(1) 在路由器 A 上，打开“路由和远程访问”控制台，右击服务器 SERVER01(本地)，选择“配置并启用路由和远程访问”选项，如图 11-7 所示。

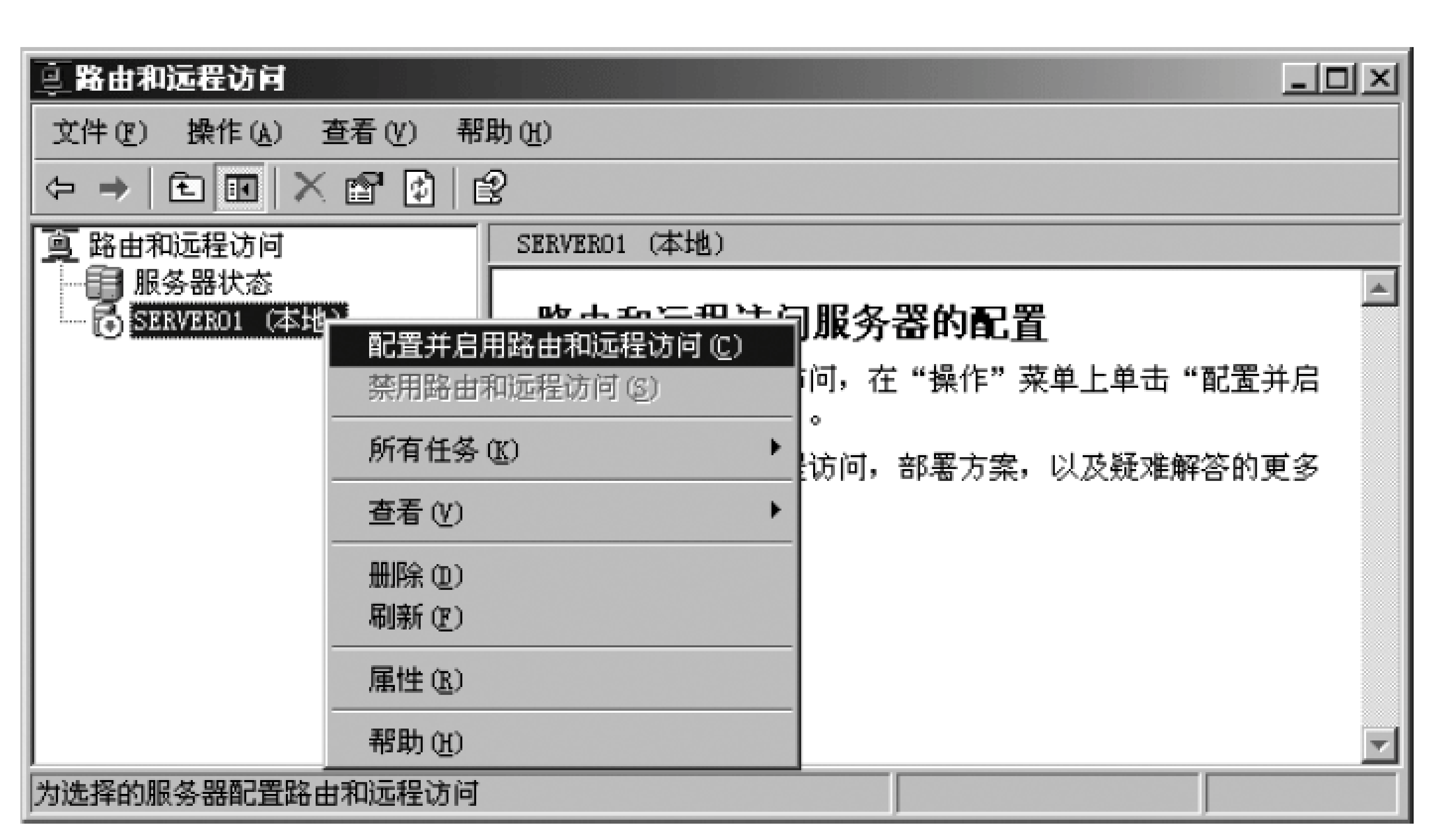


图 11-7　配置并启用路由和远程访问

(2) 在“欢迎使用路由和远程访问服务器安装向导”对话框中单击“下一步”按钮，在

图 11-8 中，选择“两个专用网络之间的安全连接”单选按钮，单击“下一步”按钮。

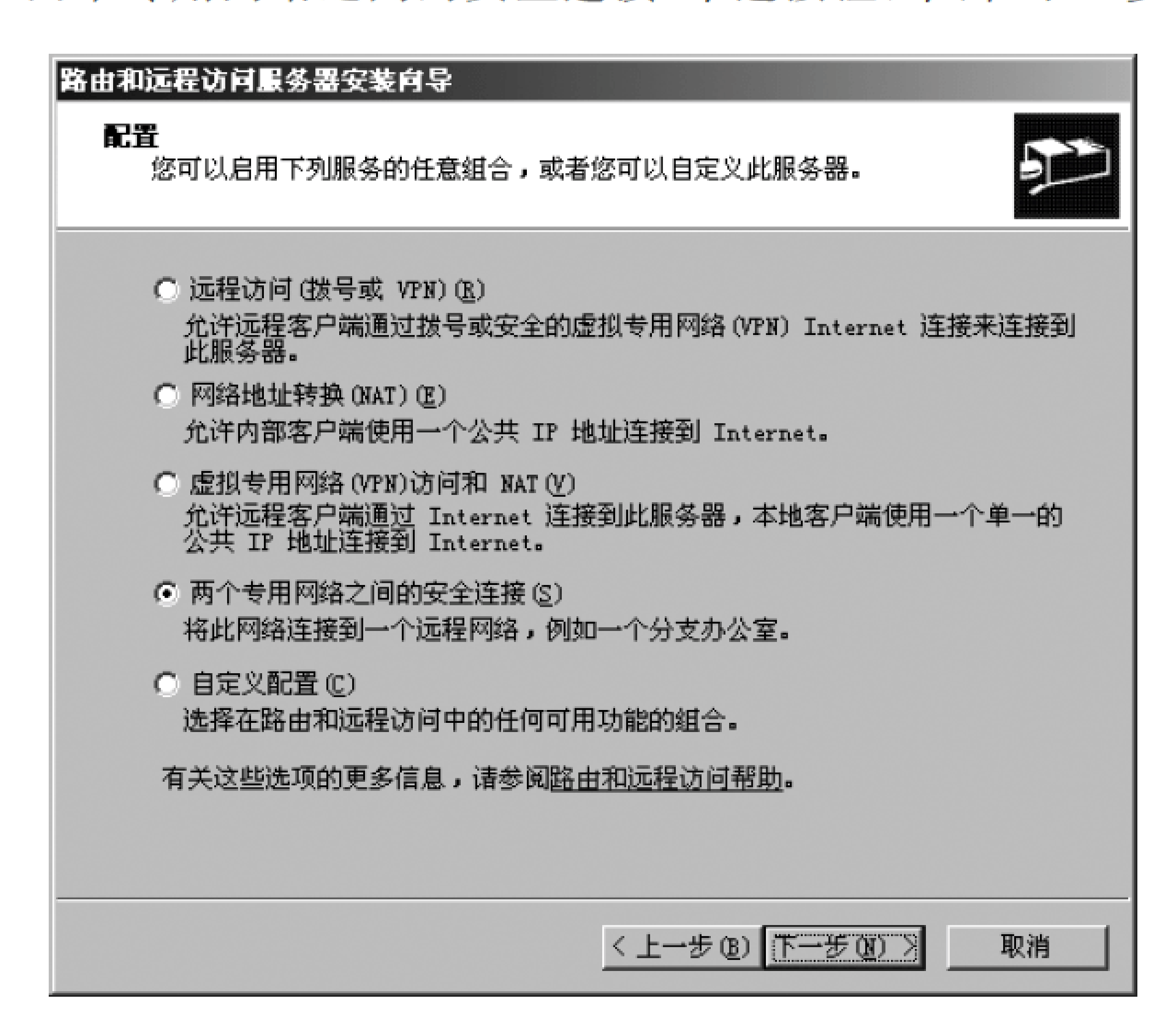


图 11-8　选择路由和远程访问的配置组合

(3) 在图 11-9 中选择“否”单选按钮，单击“下一步”按钮。



图 11-9　指定是否使用请求拨号连接

(4) 出现“完成路由和远程访问服务器安装向导”对话框时，单击“完成”按钮即可。在路由器 B 上，用同样的步骤完成上述配置。

11.2.2 检查路由表

路由器 A 安装、设置完成后，在命令提示符下，执行 route print 命令即可查看路由表。或是在“路由和远程访问”控制台中右击“静态路由”，在弹出的快捷菜单中选择“显示 IP 路由表”选项，如图 11-10 所示。



图 11-10　显示 IP 路由表

由图 11-11 可以看出，与路由器 A 直连的两个网络已经自动建立在路由器 A 的路由表内。路由器 B 的 IP 路由表有类似的输出。

SERVER01 - IP 路由表

目标	网络掩码	网关	接口	跃点数	通信协议
0.0.0.0	0.0.0.0	192.168.20.253	网段2	20	网络管理
0.0.0.0	0.0.0.0	192.168.10.253	网段1	20	网络管理
127.0.0.0	255.0.0.0	127.0.0.1	环回	1	本地
127.0.0.1	255.255.255.255	127.0.0.1	环回	1	本地
192.168.10.0	255.255.255.0	192.168.20.254	网段2	1	静态 (非请求拨号)
192.168.10.0	255.255.255.0	192.168.10.254	网段1	20	本地
192.168.10.254	255.255.255.255	127.0.0.1	环回	20	本地
192.168.10.255	255.255.255.255	192.168.10.254	网段1	20	本地
192.168.20.0	255.255.255.0	192.168.10.254	网段1	1	静态 (非请求拨号)
192.168.20.0	255.255.255.0	192.168.20.254	网段2	20	本地
192.168.20.254	255.255.255.255	127.0.0.1	环回	20	本地
192.168.20.255	255.255.255.255	192.168.20.254	网段2	20	本地
224.0.0.0	240.0.0.0	192.168.20.254	网段2	20	本地
224.0.0.0	240.0.0.0	192.168.10.254	网段1	20	本地
255.255.255...	255.255.255.255	192.168.20.254	网段2	1	本地
255.255.255...	255.255.255.255	192.168.10.254	网段1	1	本地

图 11-11　路由器 A 的 IP 路由表

在图 11-11 中，“通信协议”字段说明了此路由产生的来源。

(1) 若是通过“路由与远程访问”控制台手工建立的路由，则为静态。

(2) 若是利用 route add 命令或是在“本地连接”的 TCP/IP 中设置的，则为网络管理。

(3) 若是利用 RIP 或 OSPF 协议从其他路由器学习来的，则为 RIP 或 OSPF。

(4) 若是通过“路由和远程访问”建立过程中默认建立的路由，则为本地。

11.2.3 添加静态路由

可以通过“路由和远程访问”控制台添加静态路由，来实现数据的快速转发，静态路由经常使用在一些中、小型的网络中。

打开路由器 A 的“路由和远程访问”控制台，右击“静态路由”，选择“新建静态路由”，然后在弹出的“静态路由”对话框中输入新路由，如图 11-12 所示，表示传送给 192.168.30.0 网络的数据包，将通过“网段丙”的网络接口(即 IP 地址为 192.168.20.254 的网卡)送出，并且会传给 IP 地址为 192.168.20.253 的路由器接口(网关)，路由器的跃点数为 1。



图 11-12 新建静态路由

右击“静态路由”→“显示 IP 路由表”，可以查看新建的静态路由，如图 11-13 所示。

WIN2003-STD-VM - IP 路由表

目标	网络掩码	网关	接口	跃点数	通信协议
127.0.0.0	255.0.0.0	127.0.0.1	环回	1	本地
127.0.0.1	255.255.255.255	127.0.0.1	环回	1	本地
192.168.10.0	255.255.255.0	192.168.10.254	网段甲	10	本地
192.168.10.254	255.255.255.255	127.0.0.1	环回	10	本地
192.168.10.255	255.255.255.255	192.168.10.254	网段甲	10	本地
192.168.20.0	255.255.255.0	192.168.20.254	网段丙	10	本地
192.168.20.254	255.255.255.255	127.0.0.1	环回	10	本地
192.168.20.255	255.255.255.255	192.168.20.254	网段丙	10	本地
192.168.30.0	255.255.255.0	192.168.20.253	网段丙	1	静态(非请求拨号)
224.0.0.0	240.0.0.0	192.168.20.254	网段丙	10	本地
224.0.0.0	240.0.0.0	192.168.10.254	网段甲	10	本地
255.255.255.255	255.255.255.255	192.168.20.254	网段丙	1	本地
255.255.255.255	255.255.255.255	192.168.10.254	网段甲	1	本地

图 11-13 查看新建的静态路由

在路由器 B 上，用类似的方法，添加到 192.168.10.0 的静态路由，通过“网段丙”的网络接口(也就是 IP 地址为 192.168.20.253 的网卡)送出，并且会传给 IP 地址为 192.168.20.254 的路由器接口(网关)，路由器的跃点数为 1。

通过上述配置，路由器 A、路由器 B 上已配置静态路由，即可实现甲、乙、丙网络之间的互通。

11.3 数据包筛选器

Windows Server 2003 路由器中具有两种筛选器：请求拨号筛选器和数据包筛选器。它们的配置方式是一样的，但是作用不同，针对的接口也不同。

（1）请求拨号筛选器。只针对请求拨号接口。当路由器接收到匹配某个请求拨号接口所设置的请求拨号筛选器的 IP 数据包时，会自动初始化请求拨号连接，从而转发数据包。

（2）数据包筛选器。分为入站筛选器和出站筛选器，分别对应收到的数据包和发出的数据包。可以对任何一个物理接口配置数据包筛选器，以允许或拒绝除针对特定地址、端口和协议的通信，提高网络的安全性和灵活性。

假设有甲、乙、丙 3 个网络通过路由器 A 连接，如图 11-14 所示。为了提高各个网段之间的安全，可以在路由器的每一个网络接口上设置数据包的过滤。

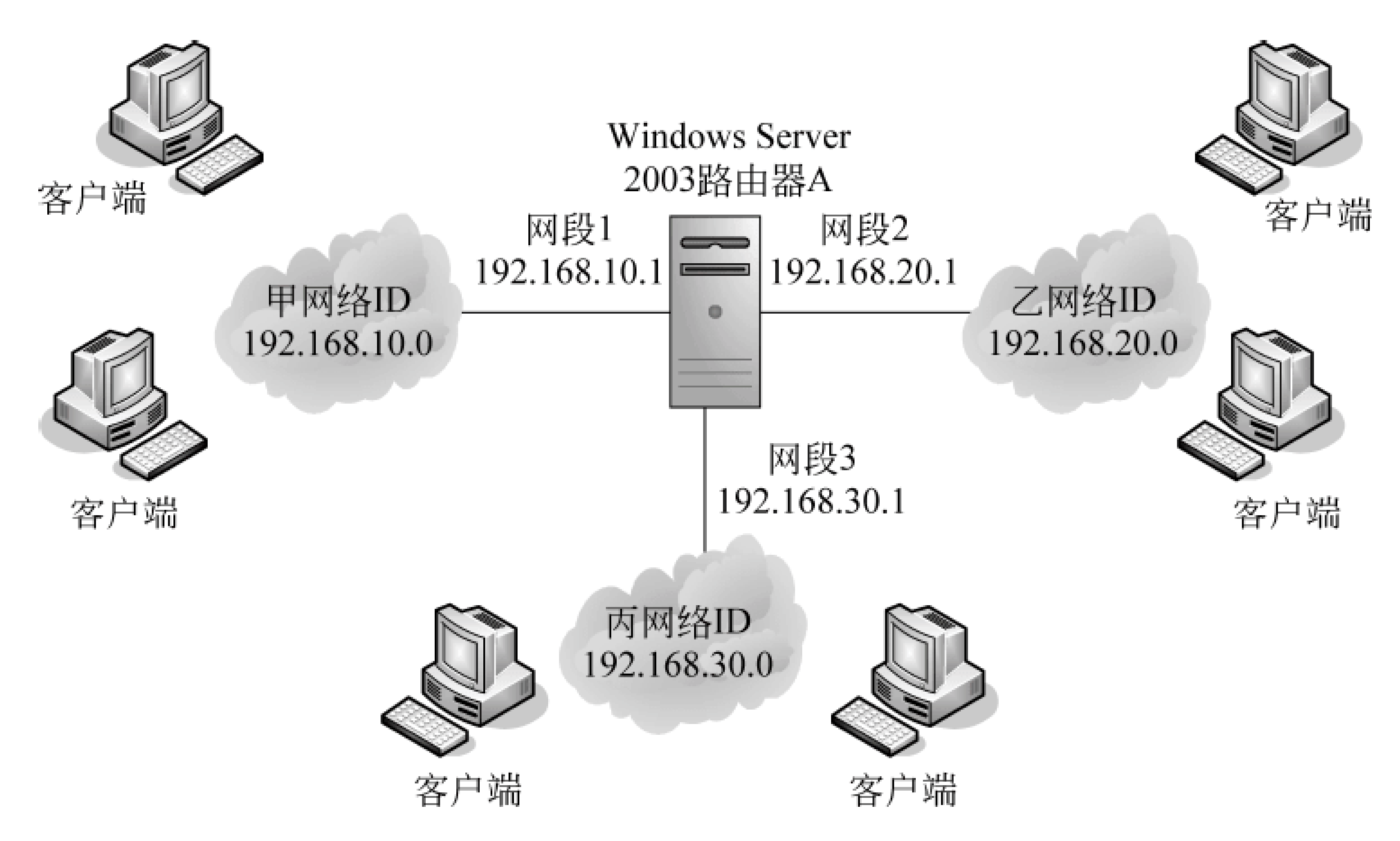


图 11-14 甲、乙、丙 3 个网络通过路由器 A 连接

（1）可以通过“入站筛选器”来设置让路由器的网络接口“网段 1”拒绝接受由甲网络内的计算机发送的 ICMP 数据包，因此甲网络内的计算机将无法利用 ping 命令来与乙、丙两个网络内的计算机通信。

（2）可以通过“出站筛选器”设置让路由器的网络接口“网段 2”拒绝发送与终端服务有关的数据包，因此甲、丙两个网络内的计算机将无法与乙网络内的终端服务器通信。

要配置数据包筛选器，操作步骤如下。

（1）在“路由和远程访问”管理控制台中，展开服务器，然后展开“IP 路由选择”，选择“常规”，右击对应的接口名，在弹出的快捷菜单中选择“属性”选项，如图 11-15 所示。

（2）在图 11-16 中，单击“入站筛选器”按钮和“出站筛选器”按钮分别进行设置。



图 11-15 设置接口的属性

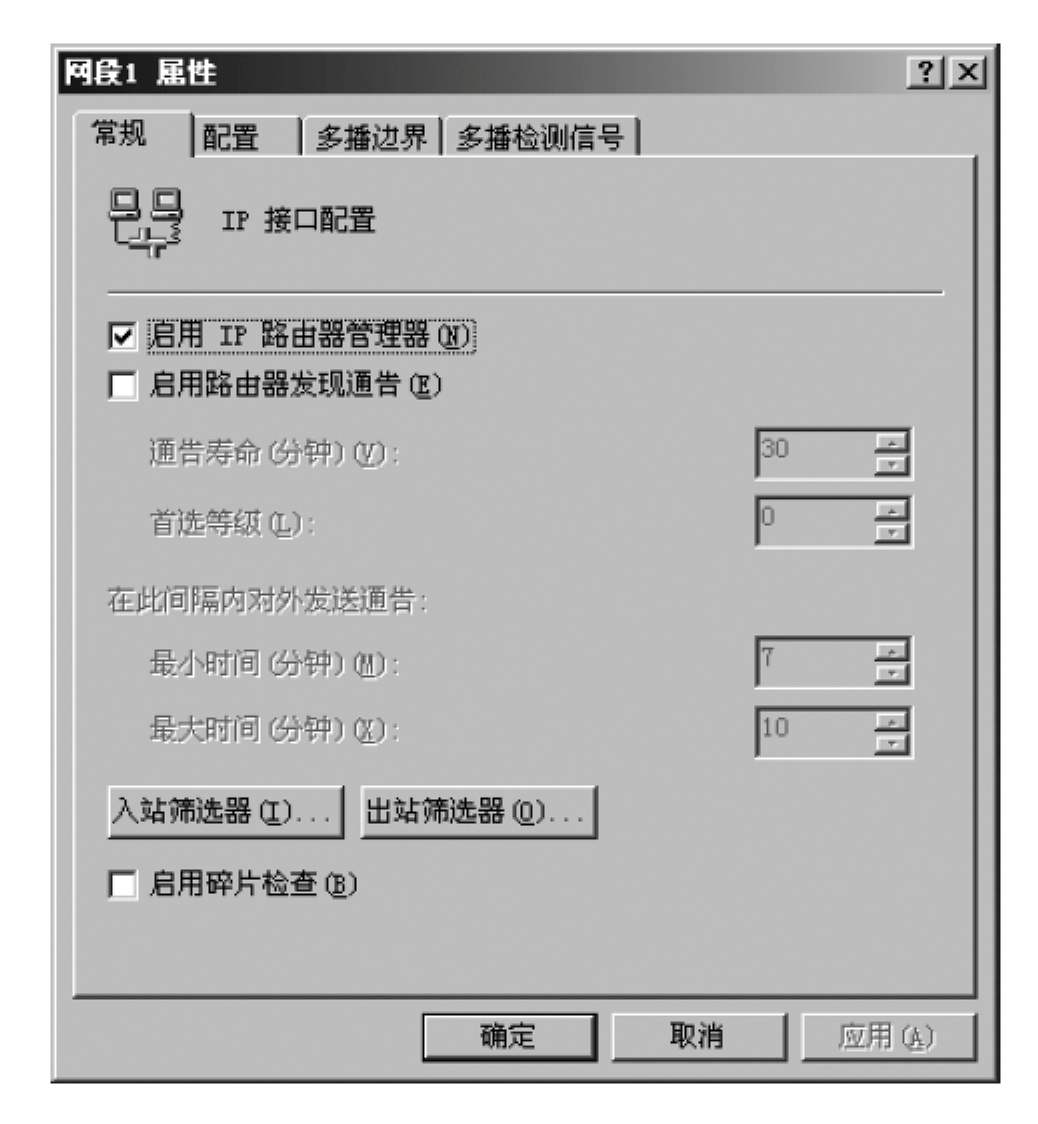


图 11-16 “网段 1”接口的属性对话框

11.3.1 入站筛选器

要设置接口“网段 1”的入站筛选器，配置甲网络内的计算机主动送出的 ICMP 数据包被拒绝，操作步骤如下。

在图 11-16 所示的对话框中，单击“入站筛选器”对话框，在入站筛选器的操作对话框中，有以下两个选项。

(1) 接收所有除符合下列条件以外的数据包。当接收到的数据包匹配下面所设置的筛选器时，丢弃此数据包，允许所有不匹配筛选器设置的数据包。

(2) 丢弃所有的包，满足下面条件的除外。当接收到的数据包匹配下面所设置的筛选器时，允许此数据包，丢弃所有不匹配筛选器设置的数据包。

根据设置筛选的要求，凡是从甲网络进入网络接口“网段 1”的 ICMP 数据包，无论其目标地址为何，都一律拒绝接收。单击“新建”按钮，定义源网络为 192.168.10.0，掩码为 255.255.255.0，目标网络不需定义，即代表所有的目标地址。协议为 ICMP，类型为 8，代码为 0，如图 11-17 所示。

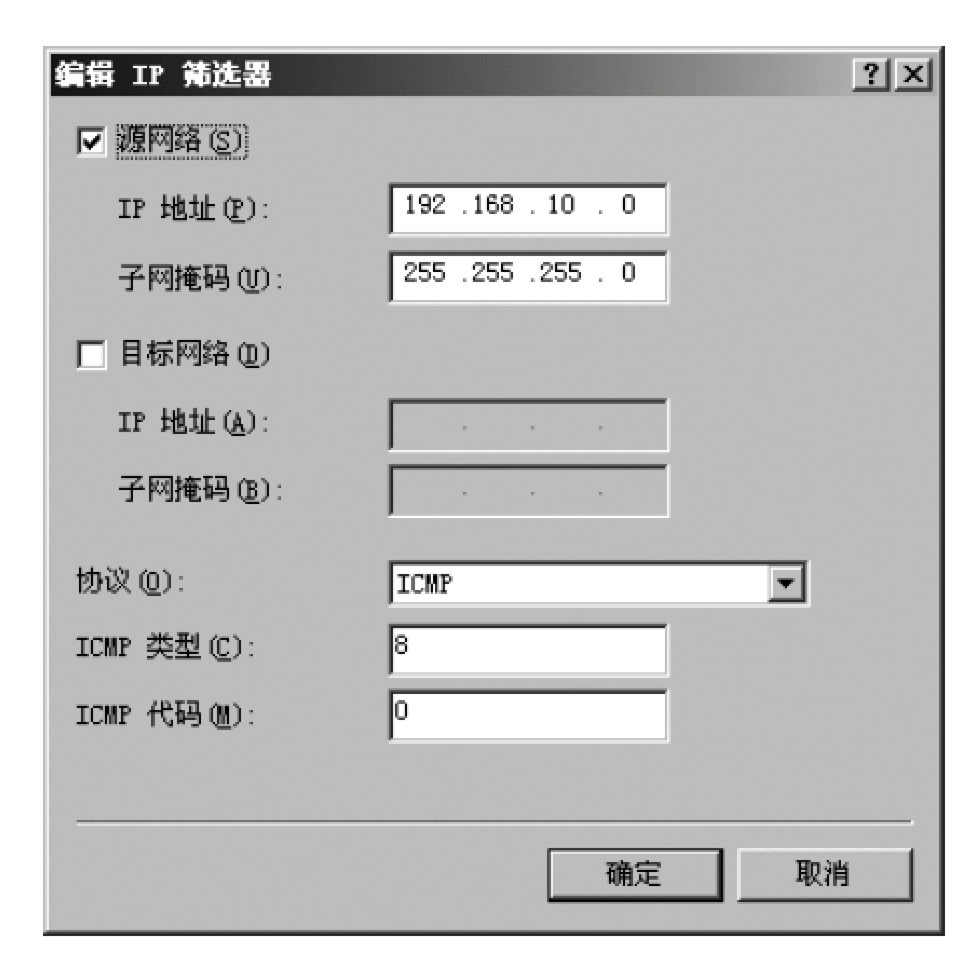


图 11-17 接口“网段 1”的入站筛选器

单击“确定”按钮，即可完成“入站筛选器”的设置，如图 11-18 所示。

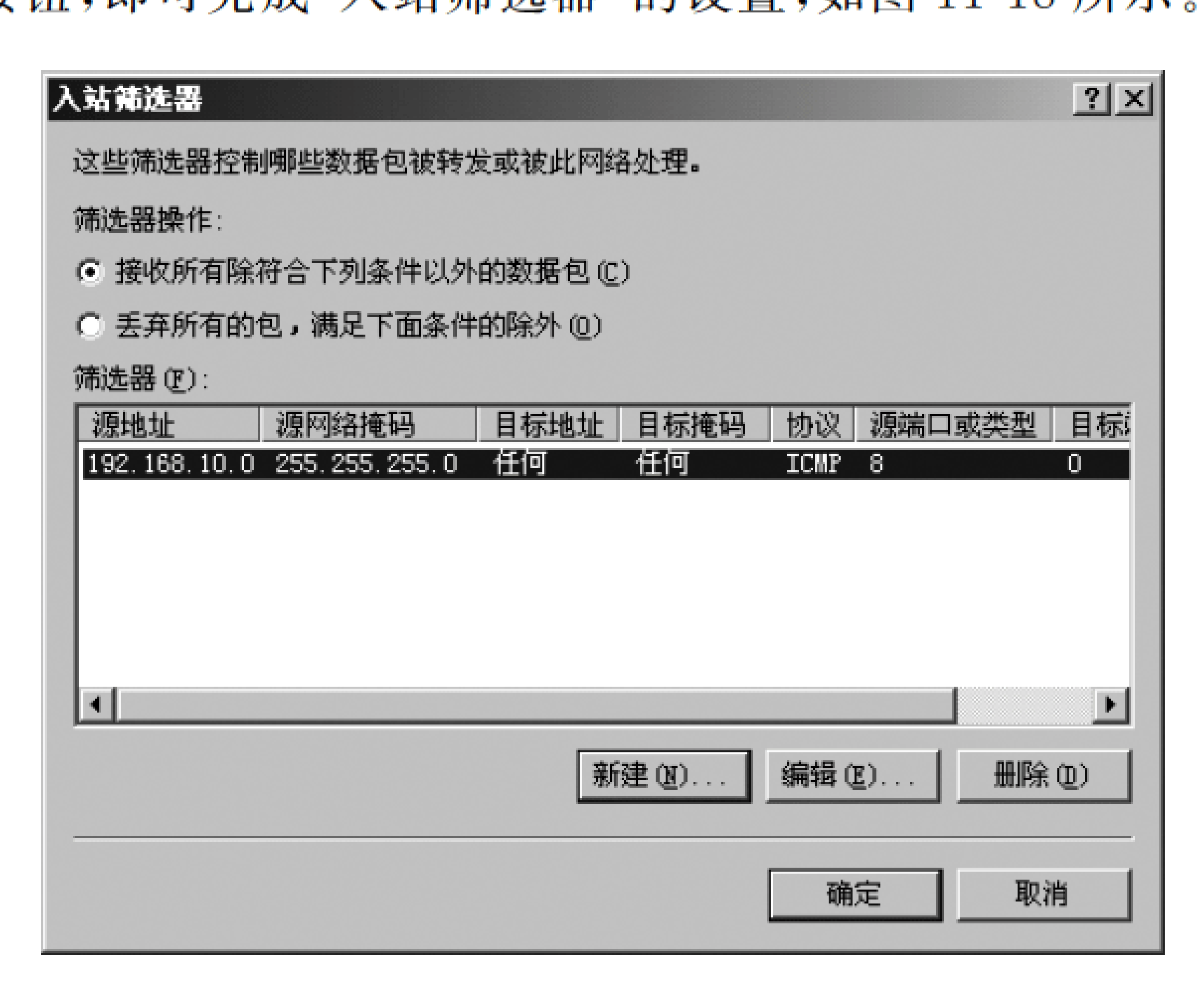


图 11-18 入站筛选器

11.3.2 出站筛选器

要设置接口“网段 2”的出站筛选器，配置甲、丙两个网络内的计算机不能与乙网络内的终端机服务器通信，操作步骤如下。

在“路由和远程访问”管理控制台中，展开服务器，然后展开“IP 路由选择”，选择“常

规”，右击接口“网段 2”，选择“属性”，在接口属性对话框的“常规”选项卡中，单击“出站筛选器”，在“筛选器操作”下选择“接收所有除符合下列条件以外的数据包”单选按钮。

根据筛选规则，路由器的网络接口“网段 2”不发送与终端服务有关的数据包，因此甲、丙两个网络内的计算机将无法利用远程桌面来连接乙网络内的终端服务器或支持远程桌面的计算机。终端服务器与远程桌面所支持的通信协议为 TCP，连接端口号为 3389。单击“新建”按钮，源网络不需定义，即代表所有的源地址，目标网络为 192.168.20.0，掩码为 255.255.255.0，源端口不用定义（值为 0），目标端口为 3389，如图 11-19 所示。

编辑 IP 筛选器
源网络(S)
IP 地址(P):
子网掩码(U):
目标网络(D)
IP 地址(A): 192 .168 . 20 . 0
子网掩码(B): 255 .255 .255 . 0
协议(O): TCP
源端口(C): 0
目标端口(N): 3389
确定 取消

图 11-19　接口“网段 2”的出站筛选器

单击“确定”按钮，即可完成“出站筛选器”的设置，如图 11-20 所示。

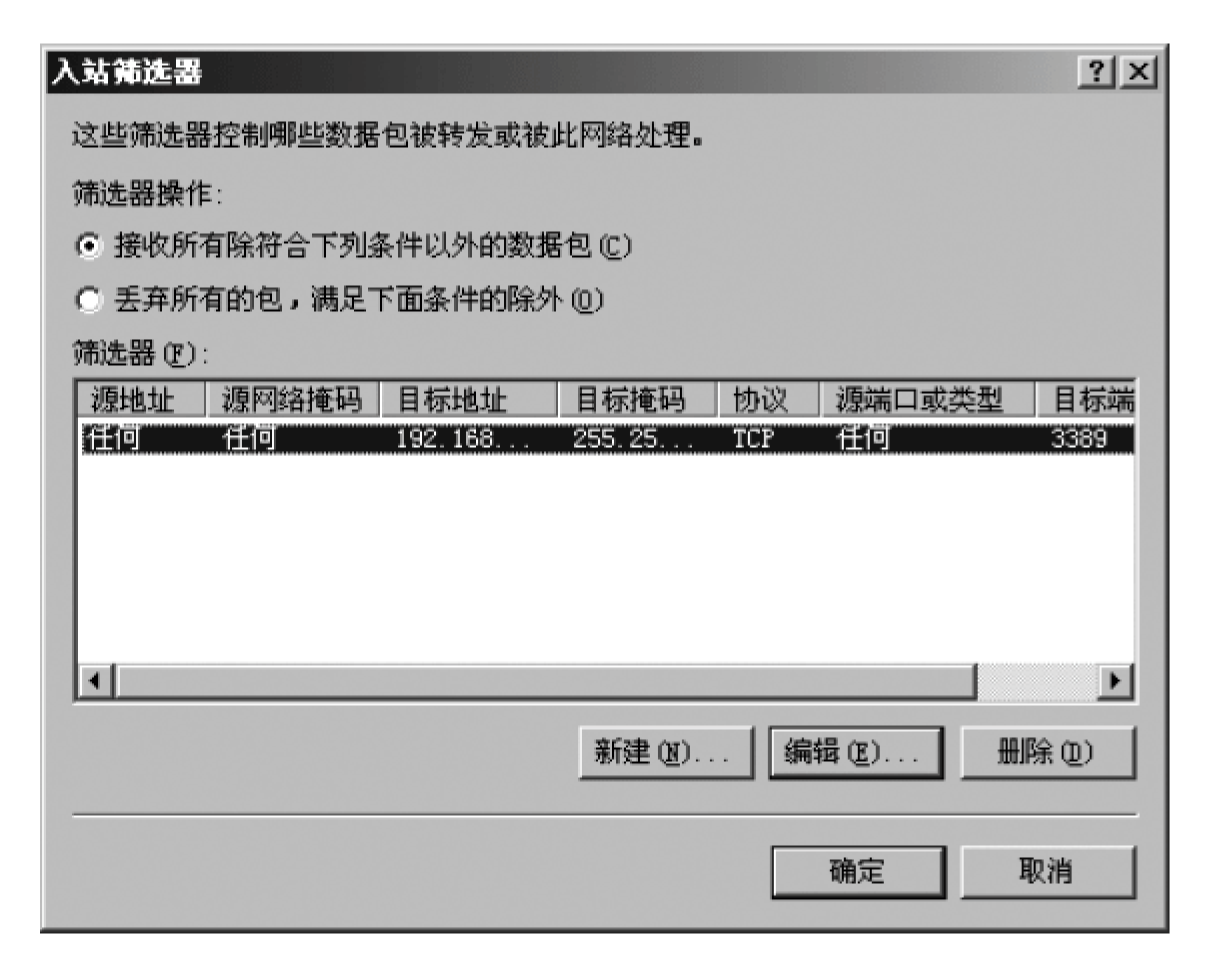


图 11-20　出站筛选器

在定义源网络和目标网络时，需要注意两点。

(1) 定义某个 IP 地址时，使用子网掩码 255.255.255.255（主机掩码）。例如，定义源

网络为 IP 地址 192.168.10.1，子网掩码为 255.255.255.255。

(2) 定义某个网络时，在子网掩码为 0 的位设置 IP 地址对应位为 0。例如，要定义网络 192.168.10.0/24，在 IP 地址处输入 192.168.10.0，子网掩码为 255.255.255.0。

11.3.3 通信协议与端口号

在配置路由器的筛选规则时，除了源网络、目标网络外，通信协议和源端口、目标端口也是匹配的条件。

每一个通信协议都有一个通信协议号。关于常用的协议号，ICMP 为 1，TCP 为 6，UDP 为 17，IGMP 为 88，OSPF 为 89 等。端口号是指 TCP/IP 中的端口，范围从 0～65 535。端口号有下列两种分类标准。

1. 按端口号范围划分

(1) 知名端口(Well-Known Ports)。范围从 0～1 023，这些端口一般固定分配给一些服务。例如，21 端口分配给 FTP 服务，25 端口分配给 SMTP 服务，80 端口分配给 HTTP 服务，135 端口分配给 RPC(远程过程调用)服务等。

(2) 动态端口(Dynamic Ports)。范围从 1 024～65 535，这些端口号一般不固定分配给某个服务，也就是说许多服务都可以使用这些端口。只要运行的程序向系统提出访问网络的申请，那么系统就可以从这些端口号中分配一个供该程序使用，在关闭程序进程后，就会释放所占用的端口号。

2. 按协议类型划分

(1) TCP 端口。即传输控制协议端口，包括 FTP 服务的 21 端口，Telnet 服务的 23 端口，SMTP 服务的 25 端口，以及 HTTP 服务的 80 端口等。

(2) UDP 端口。即用户数据包协议端口，包括 DNS 服务的 53 端口，SNMP 服务的 161 端口等。

在命令提示符下，执行“netstat -a -n”命令，就可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及状态。

11.4 动态路由 RIP

路由信息协议(Routing Information Protocols，RIP)是使用最广泛的一种距离向量路由协议，RIP 的度量标准是跳数，会优先选择跳数少的路径。RIP 支持的最大跳数是 15，跳数为 16 被认为目标网络不可到达。

11.4.1 RIP 路由概述

在图 11-21 所示的网络中，路由器 A 的路由表中没有乙网络的路由信息，路由器 B

的路由表中没有甲网络的路由信息，为了实现甲网络与乙网络之间的计算机通信，可以使用动态路由协议 RIP 来实现路由表的相互学习，实现甲网络与乙网络之间的通信。

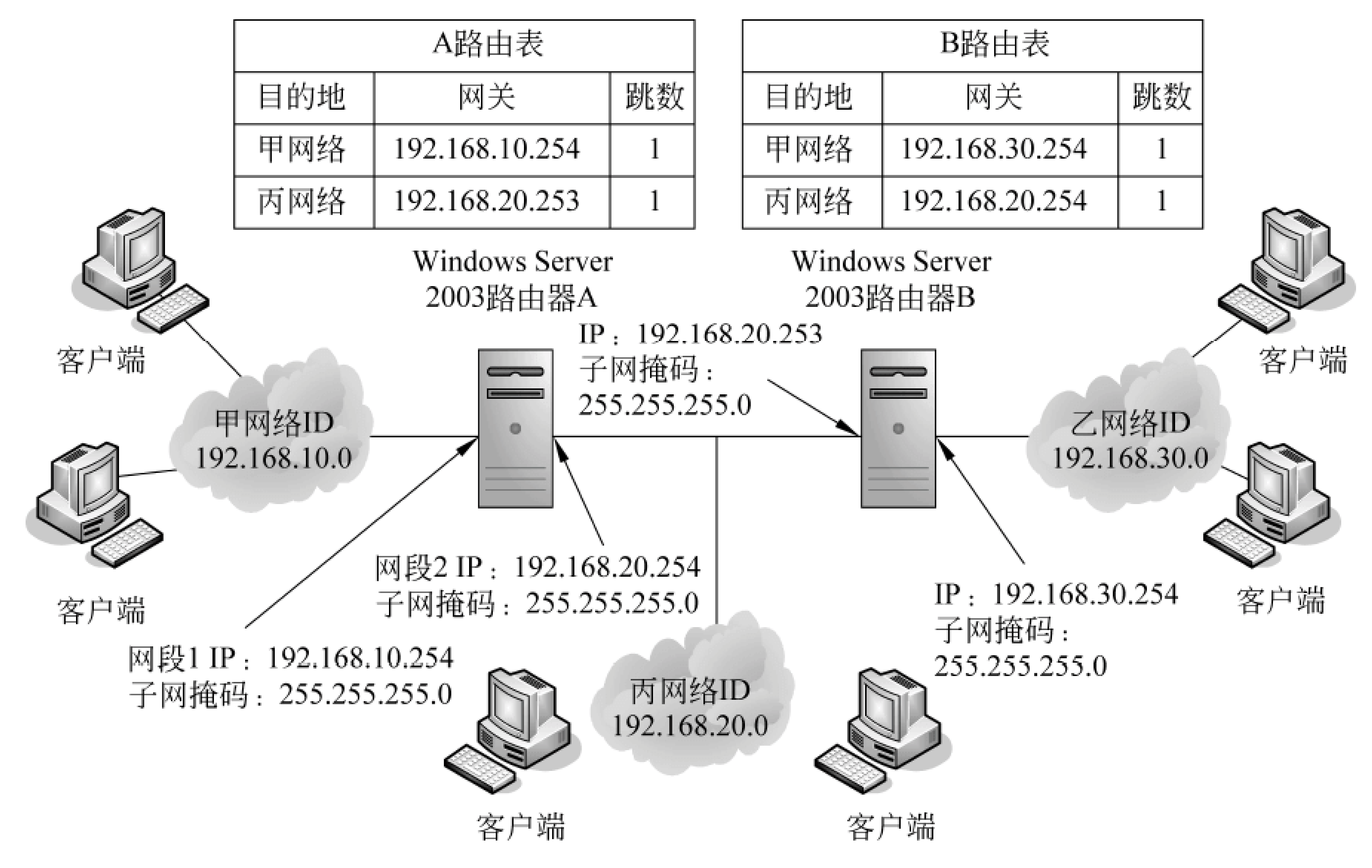


图 11-21　甲、乙、丙 3 个网络通过两台路由器连接

启用 RIP 的路由器会将其路由表内的路由信息通告给其直连的邻居路由器，而其他启用 RIP 的路由器在收到这些路由信息后，会依据这些路由信息来自动更新自己的路由表。所有的 RIP 路由器在相互学习邻居的路由表后，都可以自动建立正确的路由表。例如，路由器 A 与路由器 B 都启用 RIP 后，则路由器 A 通往乙网络的路由，路由器 B 通往甲网络的路由，都是利用 RIP 路由协议的“学习”功能得来的，如图 11-22 所示。

RIP 路由器的路由成本（即 Metric 的值）是以跳数来计算的，也就是以跨越路由器的数量来计算的。数据包传送到目的地所经过的路由器越多，表示成本越高。如果目的地是在同一网段内，则跳数算 1，之后每跨越一个路由器增加 1。

利用 Windows Server 2003 的“路由和远程访问”服务所设置的 RIP 路由器，会将所有不是通过 RIP 学习来的路由成本固定为 2，包含直连的网络路由。因此 RIP 路由器在通知相邻的其他路由器时，都会宣告这些路由成本为 2，这就是从甲网络到乙网络成本为 3 的原因。

11.4.2　启动 RIP 路由器

以图 11-21 所示的网络为例，假设已经启用了 Windows Server 2003 服务器 A、B 的路由服务。要启动 Windows Server 2003 上的 RIP 路由协议，操作步骤如下。

（1）在 Windows Server 2003 的“路由和远程访问”管理控制台中，展开服务器，展开“IP 路由选择”，右击“常规”，在弹出的快捷菜单中选择“新增路由协议”选项，如图 11-23 所示。

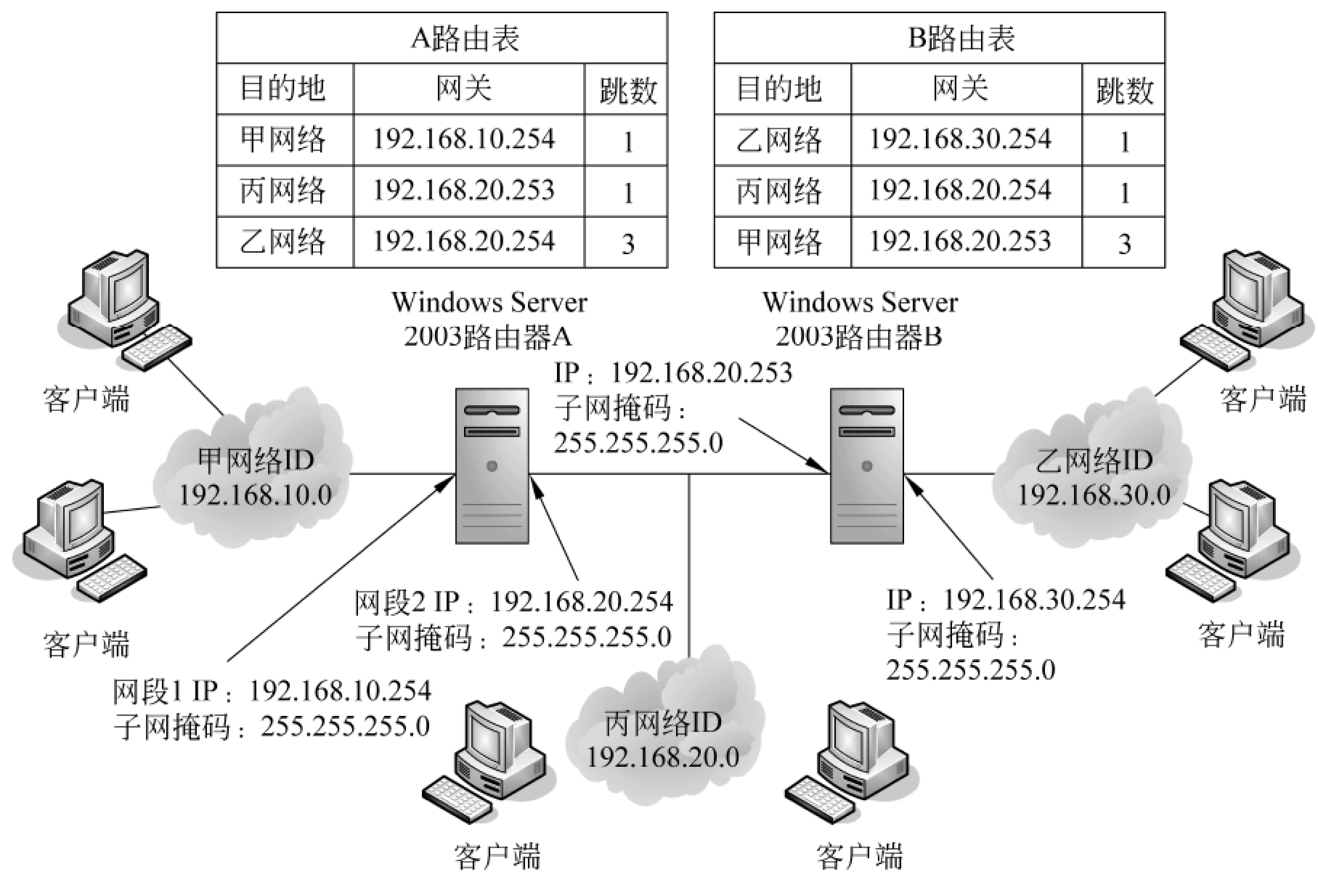


图 11-22　启用 RIP 协议的路由器



图 11-23　新增路由协议

（2）打开“新路由协议”对话框，在“路由协议”下边的文本框中选择“用于 Internet 协议的 RIP 版本 2”，如图 11-24 所示，单击“确定”按钮完成 RIP 路由协议的安装。

（3）在“路由和远程访问”管理控制台中，展开服务器，然后展开“IP 路由选择”，右击 RIP，在弹出的快捷菜单中选择“新增接口”选项，添加参与 RIP 路由更新的网络接口。只有被添加的接口才可以利用 RIP 与其他的路由器交换路由信息，如图 11-25 所示。

（4）打开图 11-26，由于要配置路由器 A 与路由器 B 进行 RIP 路由信息传递，其中“网段 1”属于甲网络，“网段 2”属于丙网络，所以选择连接“网段 2”的网络接口。



图 11-24　选择“用于 Internet 协议的 RIP 版本 2”



图 11-25　新增接口



图 11-26　选择连接“网段 2”的网络接口

（5）出现如图 11-27 所示的“RIP 属性——网段 2 属性”对话框，单击“确定”按钮。



图 11-27 “RIP 属性——网段 2 属性”对话框

（6）重复以上步骤，添加该路由器上其他的网络接口参与 RIP 路由更新，并为其他路由器安装 RIP 路由协议，使直连的网络接口也参与到 RIP 路由更新中。

11.4.3 配置 RIP 路由

为了使 RIP 路由器能够更好地与其他的 RIP 路由器通信，需要对每一个网络接口做相应的设置。以“网段 2”网络接口为例，介绍 RIP 路由的简单设置。

在 Windows Server 2003 的“路由和远程访问”管理控制台中，展开服务器，然后展开“IP 路由选择”，单击 RIP，选择“网段 2”接口，如图 11-28 所示。

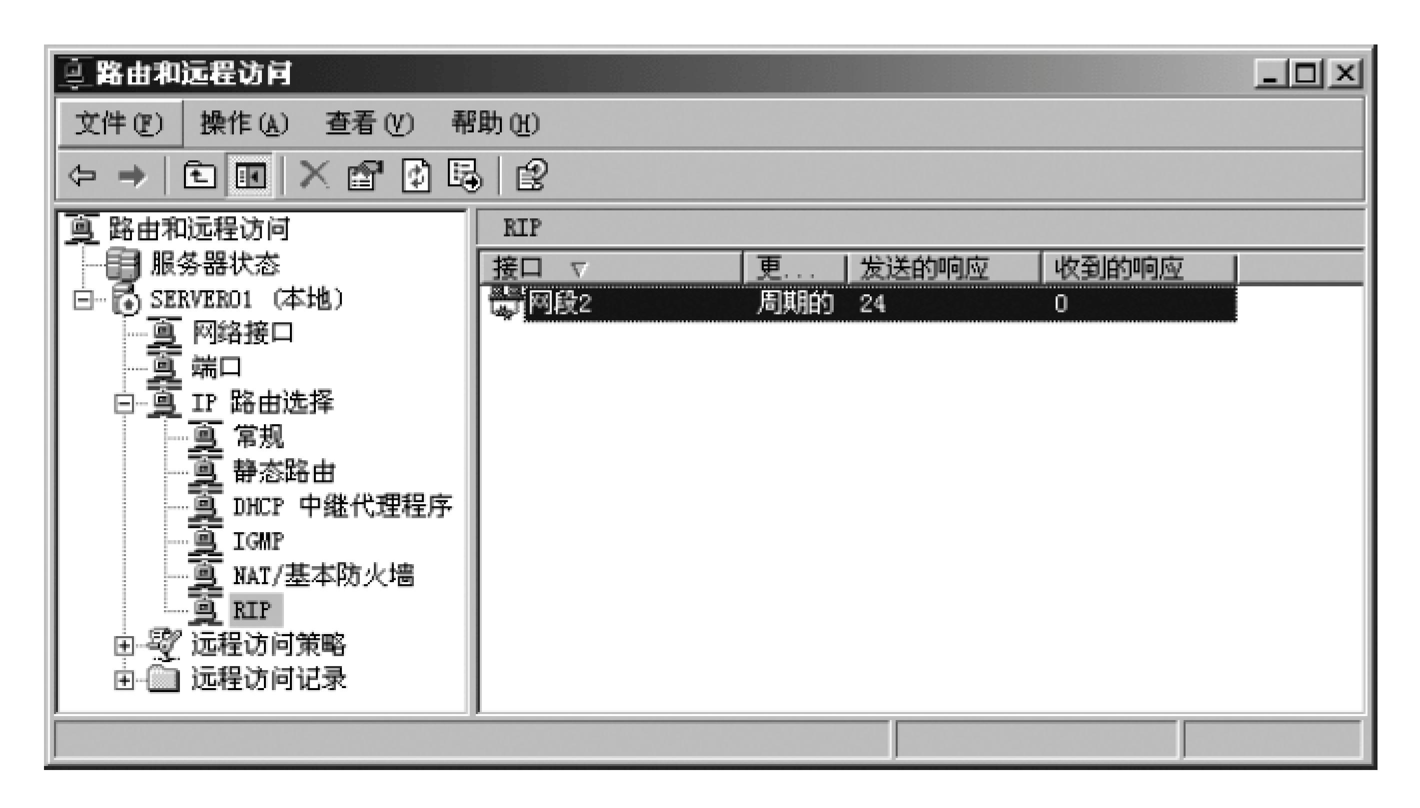


图 11-28 选择“网段 2”接口

右击“网段 2”，出现图 11-29，打开“常规”选项卡，显示路由信息协议接口的操作模

式，分为“周期性更新模式”与“自动-静态更新模式”两种。

图 11-29　“网段 2”接口 RIP 路由协议属性

（1）周期性更新模式。路由器会定期从此接口发送 RIP 路由通告，以便将其已知的路由信息传送给其他直连的路由器。而从其他路由器所学习来的路由，会在路由表内标记为 RIP 路由。这些路由信息保存在路由器的内存中，因此在路由器重新启动后丢失，但会重新开始学习。

（2）自动-静态更新模式。路由器并不会主动发送 RIP 路由通告，只是在其他路由器提出更新路由信息的要求时才会发送路由通告。而从其他路由器所学习来的路由，会在路由表内被标记为“自动静态”路由，即使路由器重新启动，这个路由也不会从路由表中清除，除非手工删除。

11.5　NAT

为了解决 IP 日益短缺的问题，网络地址转换（Network Address Translation，NAT）技术允许将多个内部地址映射为少数几个甚至一个公网地址，这样就可以实现内部网络中的主机使用私有地址透明地访问外部网络中的资源；同时外部网络中的主机也可以有选择地访问内部网络。NAT 能使内、外网隔离，提供一定的网络安全保障。

11.5.1　NAT 的网络结构

假设某公司通过 ADSL 来连接到 Internet，公司网络中有一台 Windows Server 2003 服务器，该服务器有两个网卡接口：一个用来连接公司内部局域网；另一个网卡（分配外部公网 IP 地址）连接 ADSL 调制解调器的局域网接口。在 Windows Server 2003 服务器上启用了 NAT 服务，实现公司内部网络中的计算机通过 NAT 服务器访问 Internet，如

图 11-30 所示。

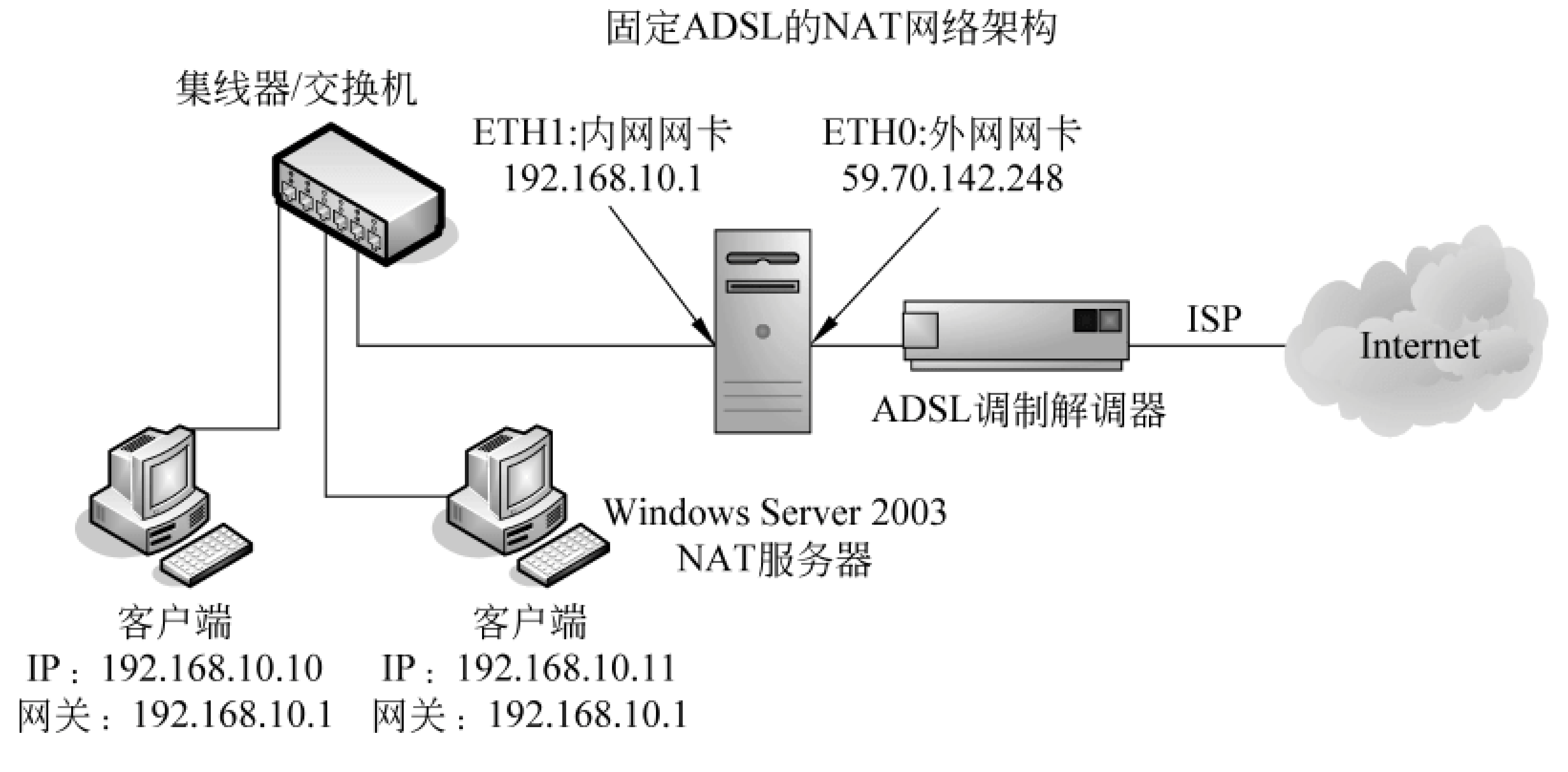


图 11-30 NAT 的网络结构

11.5.2 NAT 的工作原理

在图 11-30 所示的网络中，内部网络分配 192.168.10.0/24 网络的地址，并从 ISP 申请了一个公共的 IP 地址 59.70.142.248。当内部网中一台 IP 地址为 192.168.10.10 的客户端访问 IP 地址为 57.70.143.254 的外部 Web 服务器时，NAT 转换的过程如图 11-31 所示。

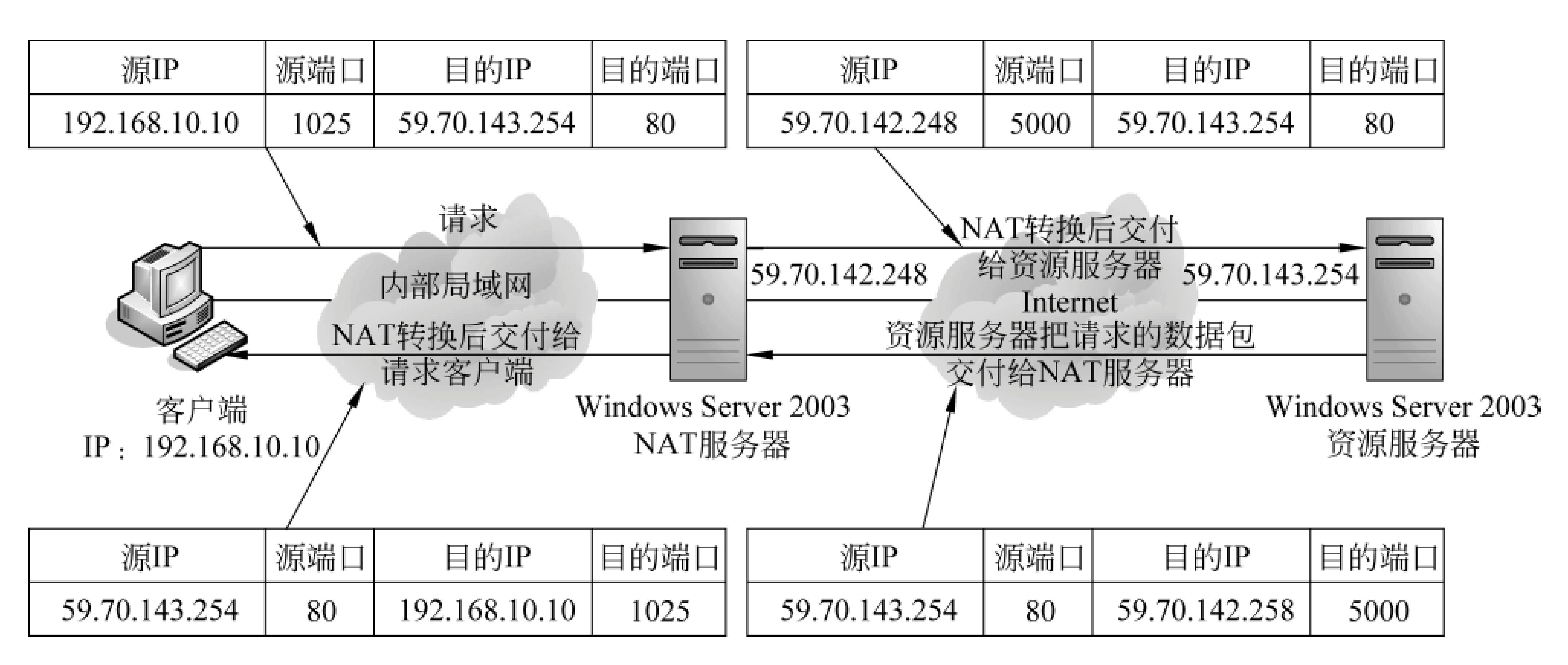


图 11-31 NAT 转换的过程

可以看出，使用 NAT 地址转换服务，对于向外发送的数据包，源 IP 地址和源 TCP/UDP 端口号将被映射到一个公共的 IP 地址和一个可能变化的 TCP/UDP 端口号。对于接收的数据包，目标 IP 地址和目标 TCP/UDP 端口号将被映射到私有 IP 地址和初始的 TCP/UDP 端口号。

使用 NAT 服务器，通过 IP 地址与端口转换，让局域网内部的客户端只要使用私网 IP 就可以上网，因此可以降低公司申请公网 IP 的成本。同时由于外网的计算机只能够

访问到 NAT 服务器的公网 IP,无法直接与局域网内的计算机通信,因此可以提高内部网的安全性。

11.5.3 安装、配置 NAT

安装、配置 NAT 服务器的操作步骤如下。

(1) 打开"路由和远程访问"控制台,右击 SEVER01(本机),在弹出的快捷菜单中选择"配置并启用路由和远程访问"选项,如图 11-32 所示。

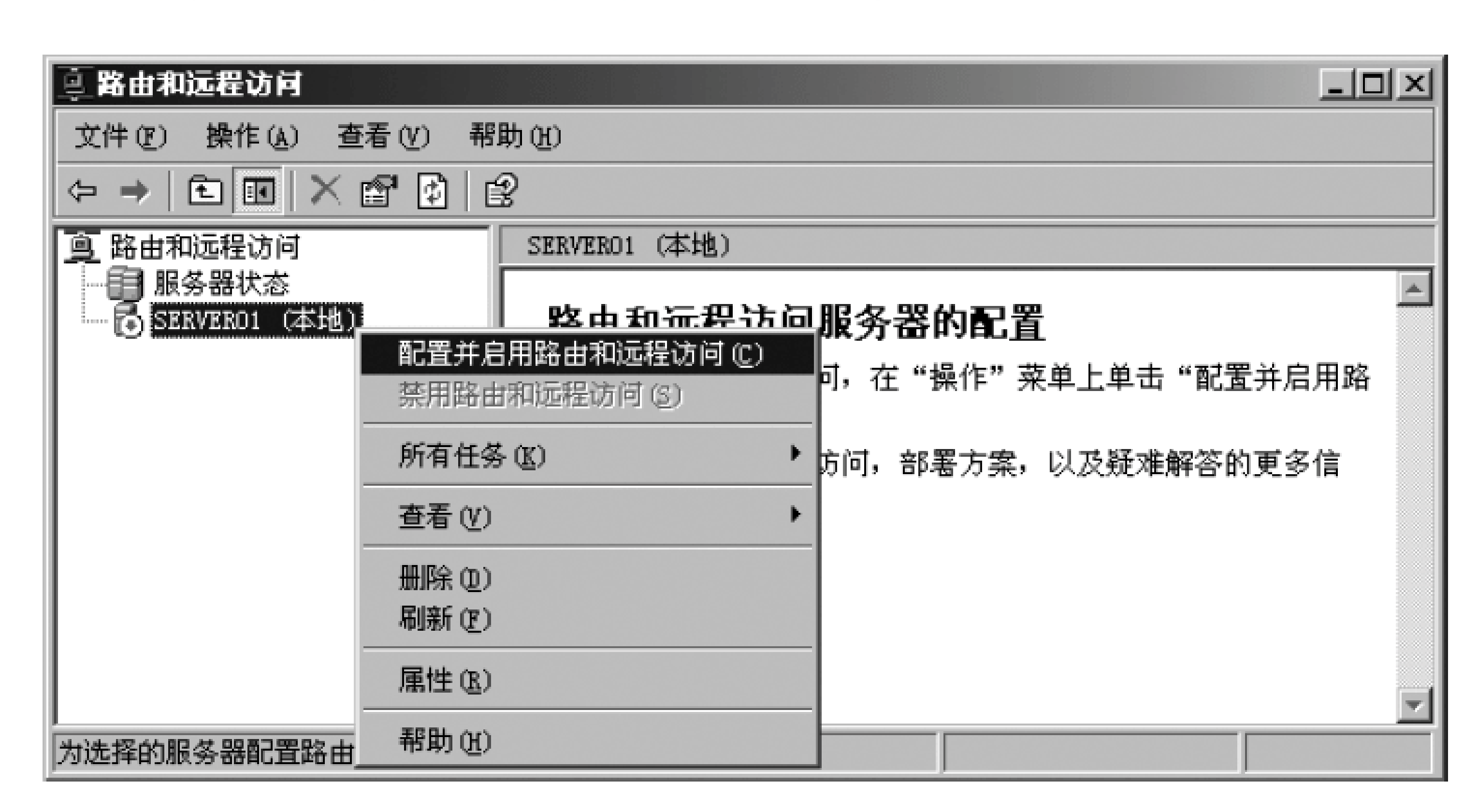


图 11-32 配置并启用路由和远程访问

(2) 在"欢迎使用路由和远程访问服务安装向导"对话框中,单击"下一步"按钮。在图 11-33 中,选择"网络地址转换(NAT)"单选按钮。

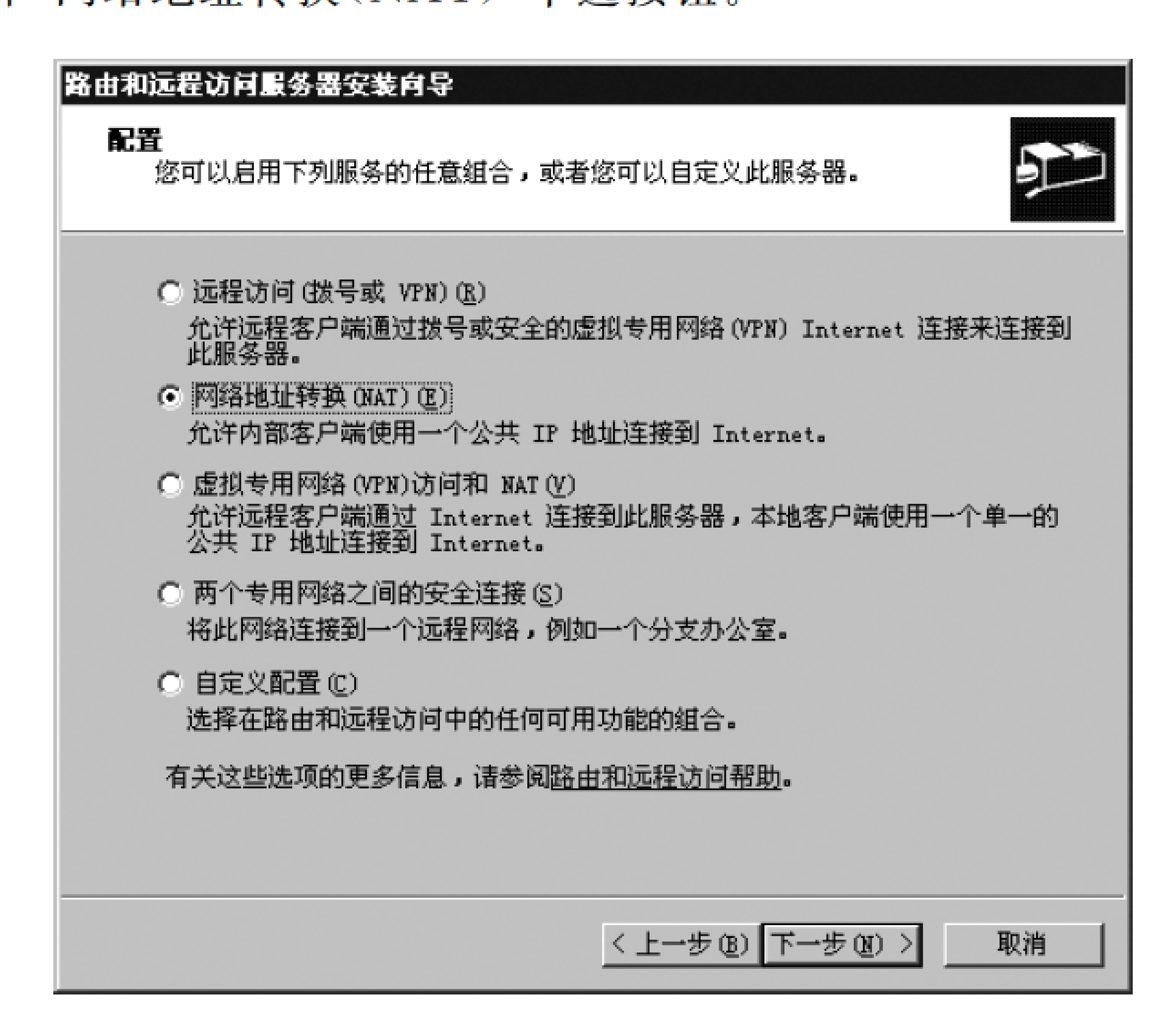


图 11-33 选择网络地址转换(NAT)

(3) 单击"下一步"按钮,选择用来连接 Internet 的网络接口,这里选择 IP 地址为

59.70.142.248 的“Eth0 外网网卡”，系统默认会启动基本防火墙，如图 11-34 所示。

路由和远程访问服务器安装向导
NAT Internet 连接
您可以选择一个现存的接口，或者为客户端计算机创建一个新的请求拨号接口来连接到 Internet。
使用此公共接口连接到 Internet(U):

名称	描述	IP 地址
内部网卡ETH1	VMware Virtual E...	192.168.10.1
外部网卡ETH0	Realtek RTL8139 ...	59.70.142.248

创建一个新的到 Internet 的请求拨号接口(D)
当客户端使用 Internet 时激活请求拨号接口。如果此服务器连接到一个调制解调器或使用通过以太网的点对点协议，则选择此选项。请求拨号接口向导将在此向导结束后启动。
通过设置基本防火墙来在对选择的接口进行保护(E)
基本防火墙防止未授权的用户通过 Internet 访问此服务器。
有关网络接口的更多信息，请参阅路由和远程访问帮助。
< 上一步(B) 下一步(N) > 取消

图 11-34 选择连接 Internet 的网络接口

(4) 单击“下一步”按钮，如果 NAT 服务器检测不到网络中有 DHCP 或 DNS 服务器，则会弹出如图 11-35 所示的“名称和地址转换服务”对话框，即如何对客户端提供 IP 地址及 DNS 解析。有两种选择。

① 启用基本的设置名称和地址服务。指利用路由和远程访问服务本身的 DHCP 分配器和 DNS 代理，自动为 NAT 客户端提供分配 IP 地址和 DNS 解析服务。

② 我将稍后设置名称和地址服务。指网络管理员配置好 NAT 服务后，再设置 DHCP 服务和 DNS 服务。

在此选择“启用基本的名称和地址服务”单选按钮，单击“下一步”按钮。

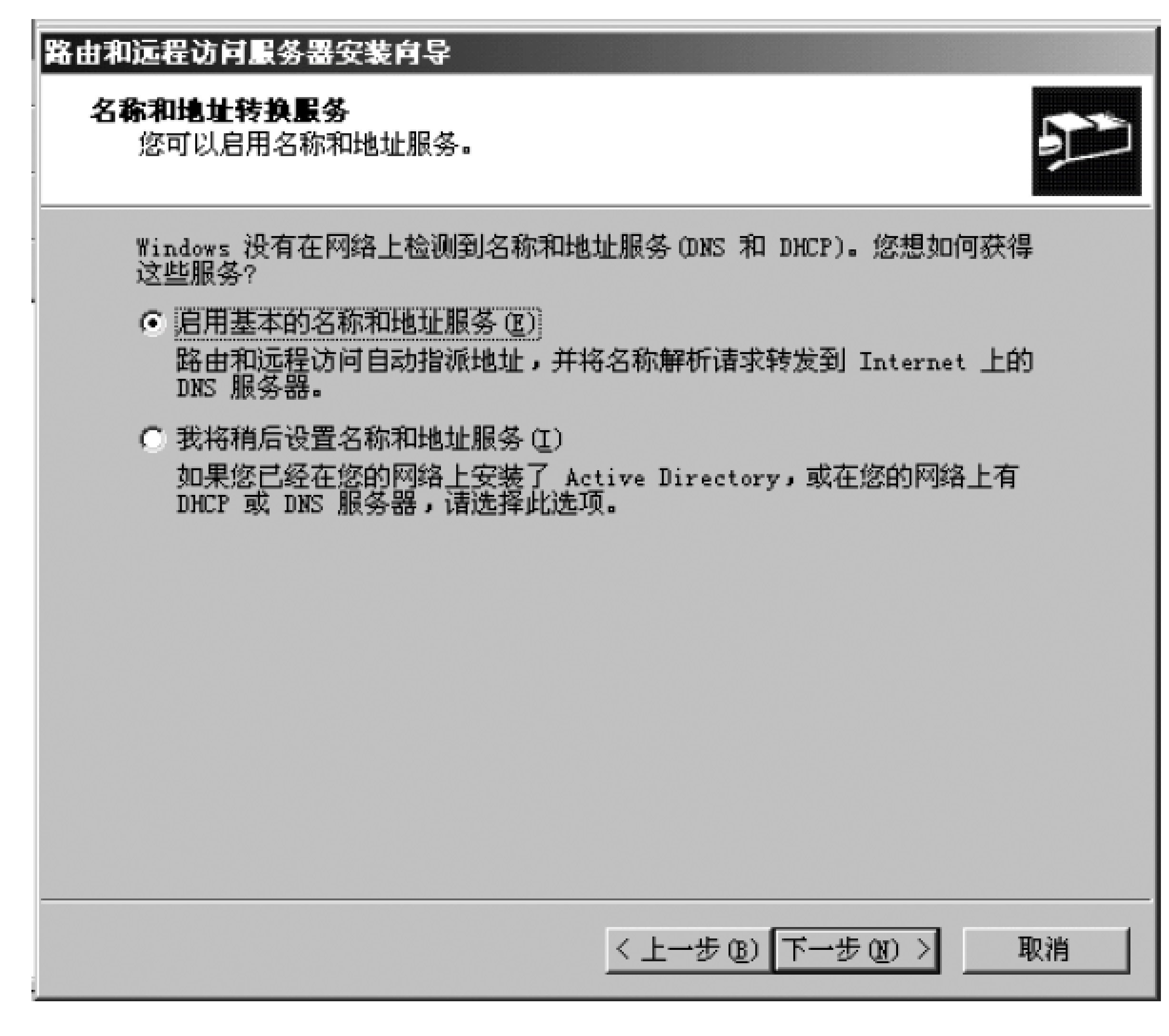


图 11-35 启用基本的名称和地址服务

(5) 如果由 NAT 服务器分配 IP 地址的话，它会分配网络 ID 为 192.168.10.0 的 IP 地址给客户端，如图 11-36 所示，单击“下一步”按钮。

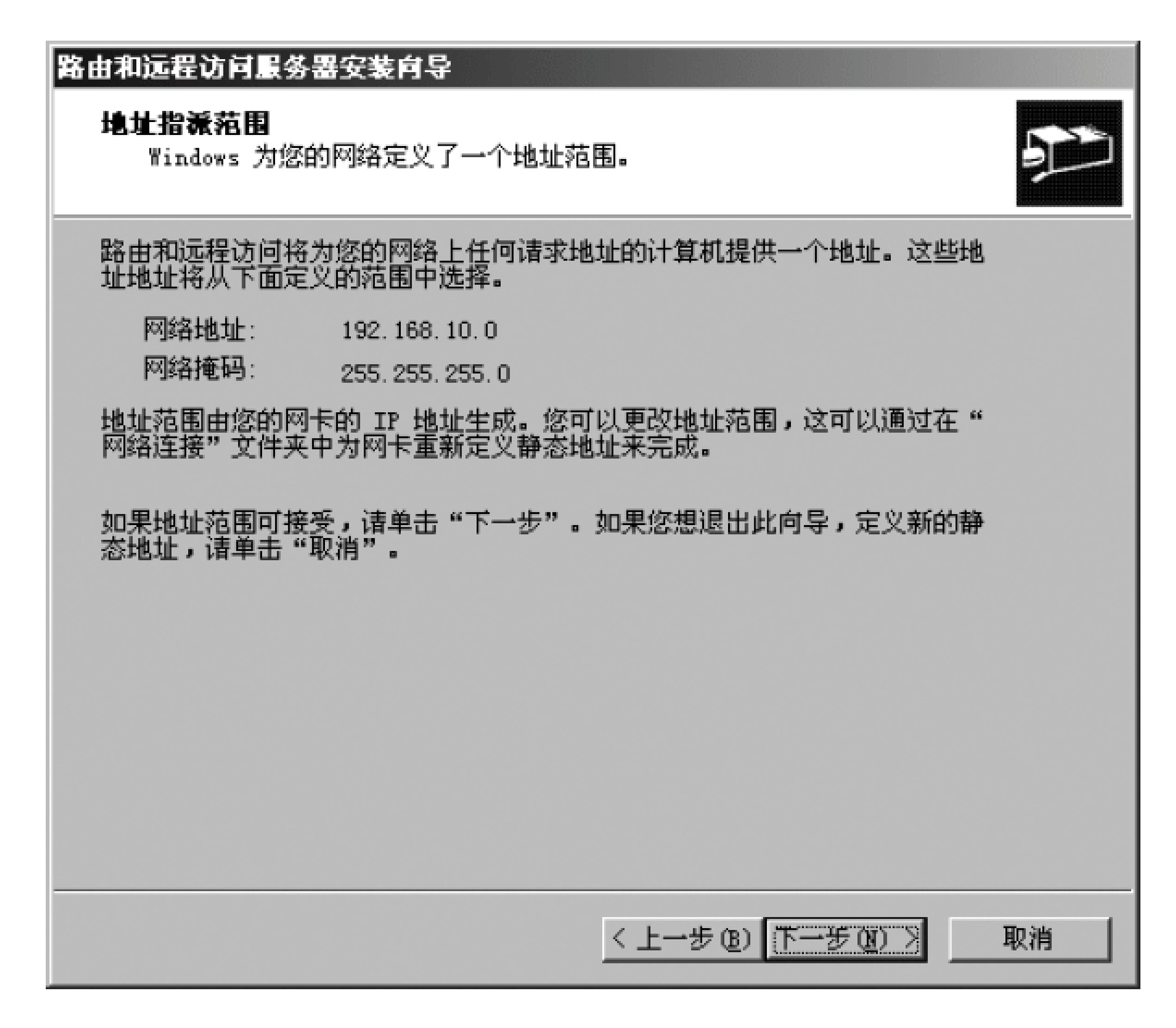


图 11-36　指派网络 ID 为 192.168.10.0 的 IP 地址

(6) 出现“完成路由和远程服务安装向导”对话框时，单击“完成”按钮即可完成 NAT 服务的基本设置。

11.6　DHCP 分配器与 DNS 代理

NAT 服务器本身提供了两个功能，可以实现客户端 IP 地址的分配和名称解析，这两个功能分别如下。

(1) DHCP 分配器。用来分配 IP 地址给内部网中的客户端计算机。

(2) DNS 代理。可以为内部网的计算机提供名称解析服务。

11.6.1　DHCP 分配器

DHCP 分配器的作用类似于 DHCP 服务器，用来分配 IP 地址给内部网中的客户端计算机。在设置 NAT 服务器时，如果系统检测到网络上有 DHCP 服务器，它就不会激活 DHCP 分配器。而是优先使用 DHCP 服务器提供的服务。

要启动、修改 DHCP 分配器的设置，可以在“路由和远程访问”控制台中选择服务器，并选择“IP 路由选择”，右击“NAT/基本防火墙”，选择“属性”，在打开的“NAT/基本防火墙属性”对话框中，选择“地址指派”选项卡，如图 11-37 所示。

DHCP 分配器分配给客户端的 IP 地址范围是 192.168.10.1～192.168.10.254，这个默认值是根据 NAT 服务器局域网接口的 IP 地址产生的。可以修改这个设置值，不过必须与 NAT 服务器局域网接口的 IP 地址在同一网络。NAT 的 DHCP 分配器只能分配

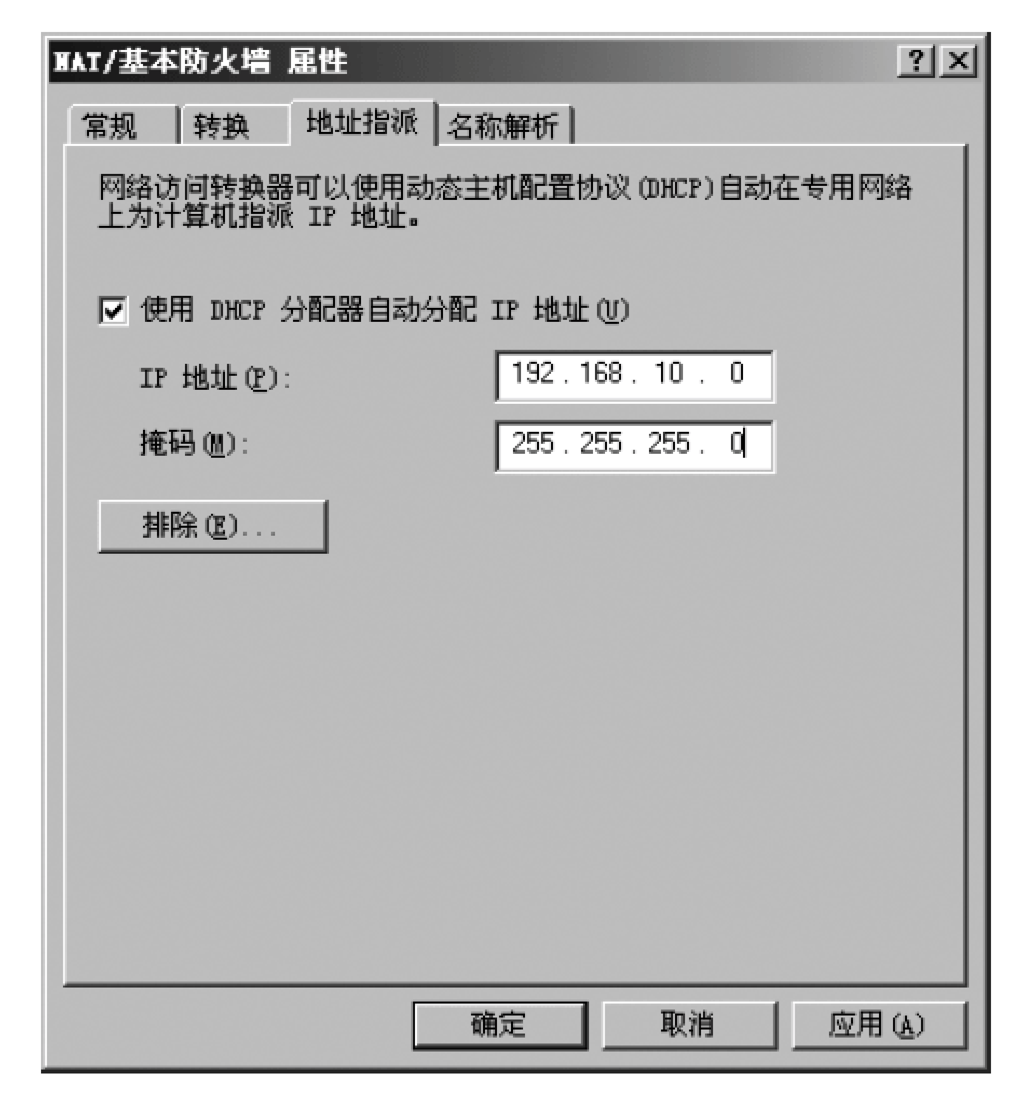


图 11-37　NAT/基本防火墙的“地址指派”选项卡

一个网段的 IP 地址，如果 NAT 服务器有多个专用接口(也就是连接多个子网)，就必须通过 DHCP 服务器来分配 IP 地址。

11.6.2　DNS 代理

要为内部网络中的客户端计算机提供 DNS 代理名称解析服务，需要启动、配置 DNS 代理，操作步骤如下。

打开“路由和远程访问”控制台，选择服务器，并选择“IP 路由选择”，右击“NAT/基本防火墙”，选择“属性”，选择“名称解析”选项卡，如图 11-38 所示。



图 11-38　NAT/基本防火墙的“名称解析”选项卡

选取“使用域名系统(DNS)的客户端”复选框,表示要启用 DNS 代理的功能,以后只要客户端上网、收发电子邮件等,NAT 服务器都会代替这些客户端来向 DNS 服务器查询网站、邮件服务器等主机的 IP 地址。在查询过程中,NAT 服务器会向本机在 TCP/IP 设置处所指定的 DNS 服务器查询。如果这些 DNS 服务器位于 Internet,则可以选取“当名称需要解析时连接到公用网络”复选框;如果是拨号连接,然后利用 PPPoE 指定拨号“远程路由器”来连接 Internet。

11.7 NAT 服务器内的防火墙

配置好 NAT 服务器之后,内部网络中的主机可以访问外部网络,但由于 NAT 服务本身具有防火墙的作用,默认外部网络的主机不能访问内部网络。有时内部网络需要对外提供服务,就需要打开 NAT 服务器内的防火墙,这里主要介绍端口映射和地址映射技术,实现在使用 NAT 的内部网络中能够对外提供服务。

11.7.1 NAT 网络接口与防火墙

设置 NAT/基本防火墙的操作步骤如下。

打开“路由和远程访问”控制台,展开服务器,展开“IP 路由选择”下的“NAT/基本防火墙”,选中需要设置的网络接口,右击“属性”,打开“NAT/基本防火墙”选项卡,只有对外连接的公用接口才可以启用基本防火墙,对内的专用接口无法启用基本防火墙,如图 11-39 所示。

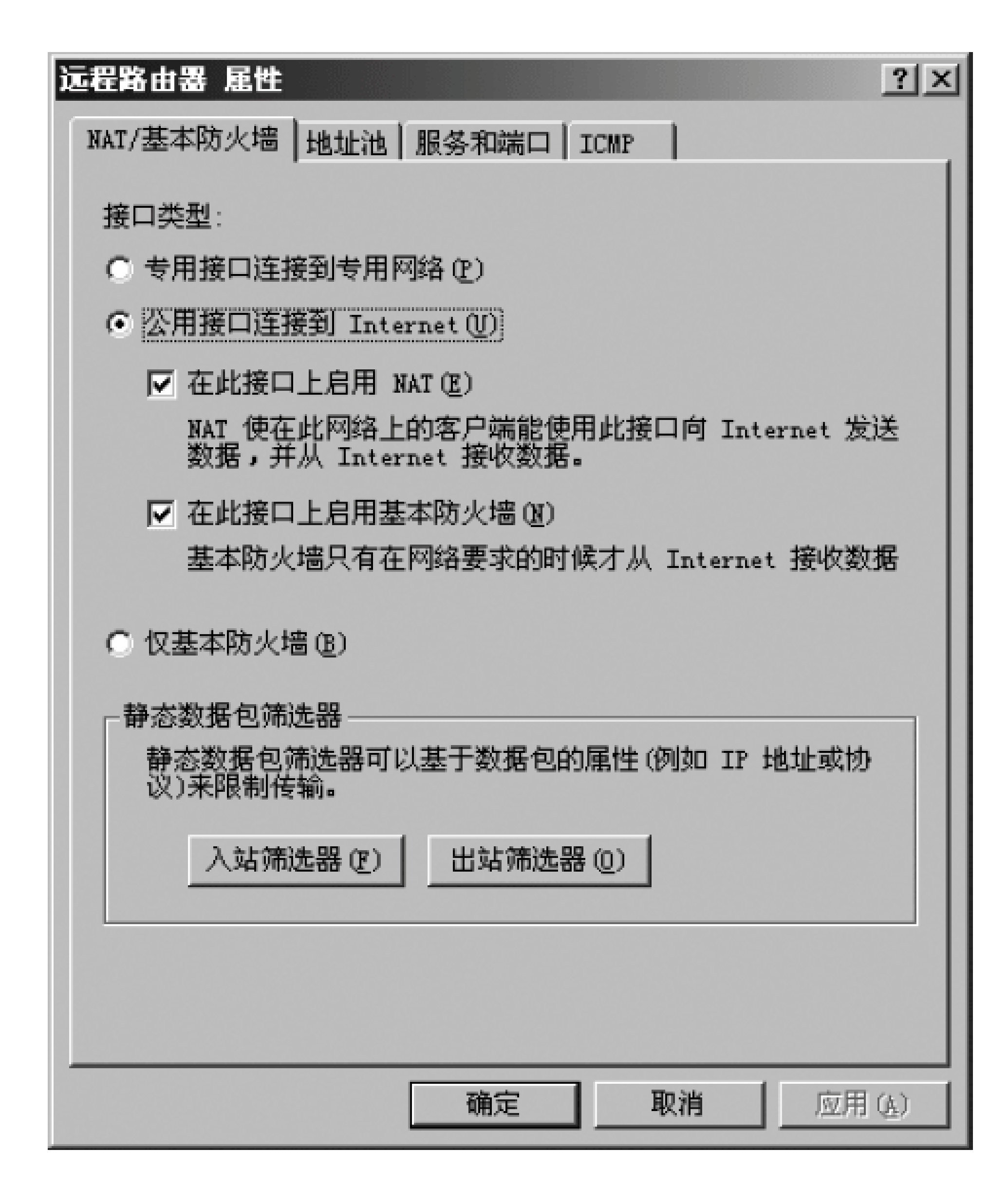


图 11-39 “NAT/基本防火墙”选项卡

(1) 专用接口到专用网络。如果接口用来连接内部局域网,则选择此单选按钮。

(2) 公用接口连接到 Internet。如果接口用来连接 Internet,则选择此选项,并且可以选择是否要启用 NAT 与基本防火墙的功能。

(3) 基本防火墙。表示此接口将只提供基本防火墙的功能,不提供 NAT 的功能。

Windows Server 2003 的 NAT 与基本防火墙具备静态数据包筛选功能,通过单击图 11-39 中的"入站筛选器"与"出站筛选器"按钮可以自行设置静态数据包筛选的规则,提高内部网络的安全性。

11.7.2 端口映射

默认情况下,NAT 服务只为内部网络中的计算机提供访问外部网络的能力,而不允许外部网络中的计算机访问内部网络中的计算机,因为内部网络中的计算机使用的是私有 IP 地址。如果在内部网络中创建了 Web 网站、FTP 站点、电子邮件服务等,要想让外部网络的用户来访问这些服务,可以通过端口映射技术,就可以对外提供内部局域网提供的这些服务。

假设内部网中一台计算机 A 上有 Web 网站,其 IP 地址为 192.168.10.2,Web 服务默认的端口为 80,如果要让外部网络中的用户可以访问此 Web 网站,则需要对外宣布 Web 网站的 IP 地址为 59.70.142.248(即 NAT 服务器上连接外部网络接口的 IP 地址),当有外部的用户通过 http://59.70.142.248 来访问此网站时,NAT 服务器会将此请求传送到内部的计算机 A,并由计算机 A 上的 Web 网站来负责处理用户的请求。该 Web 网站将用户请求的内容传送给 NAT 服务器,再由 NAT 服务器负责传送给外部用户的计算机,如图 11-40 所示。

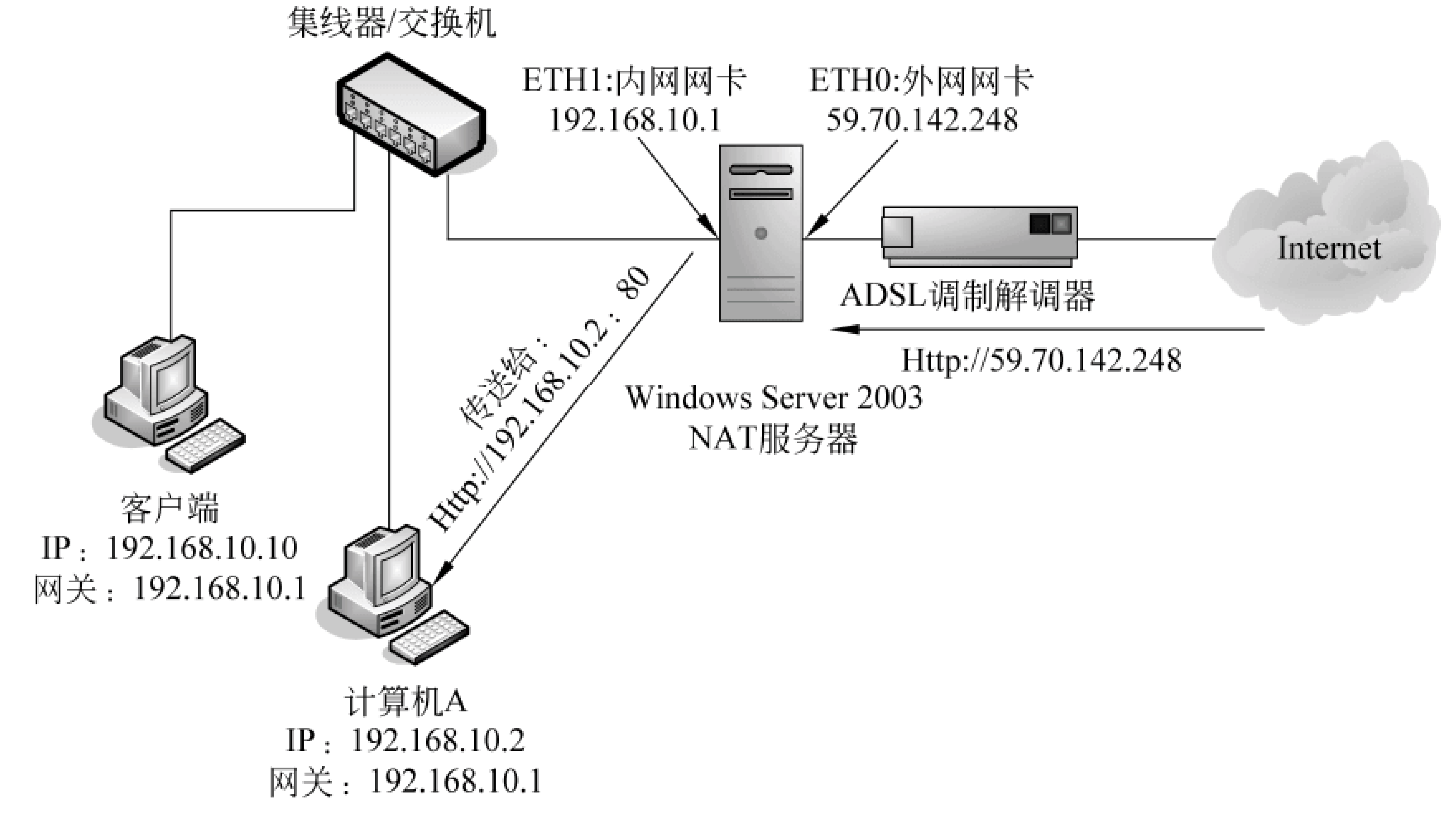


图 11-40 NAT 端口映射

要设置 TCP/UDP 端口映射,操作步骤如下。

打开“路由和远程访问”控制台，展开“服务器(本地)”，展开“IP 路由选择”下的“NAT/基本防火墙”，双击连接外部网络的网络接口，打开“服务和端口”选项卡，从“服务”列表中选取要对外提供的服务，如图 11-41 所示。

由于要对外提供 Web 服务，因此选中“Web 服务器(HTTP)”复选框，在弹出的图 11-42 中进行设置。

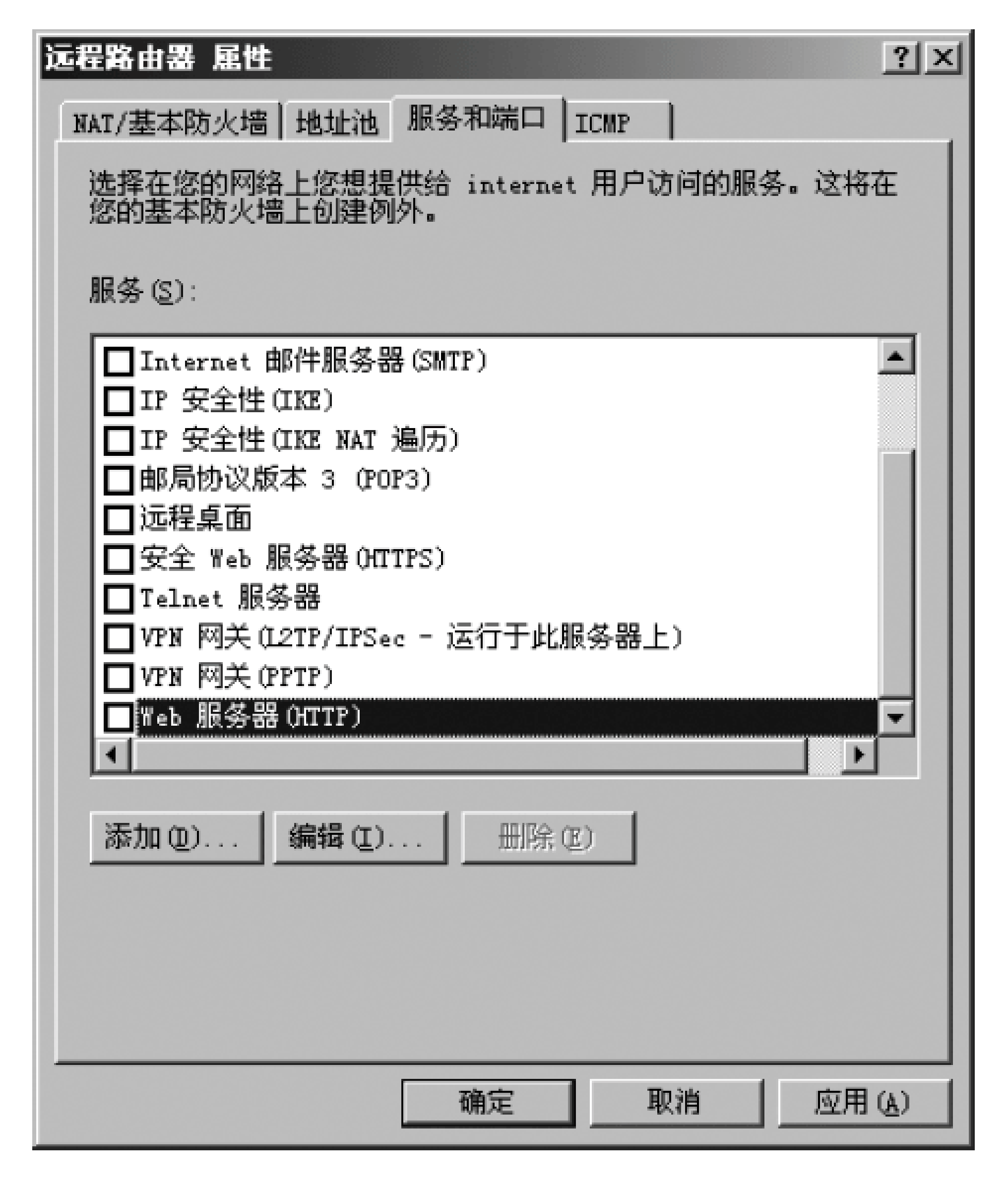


图 11-41 “服务和端口”选项卡

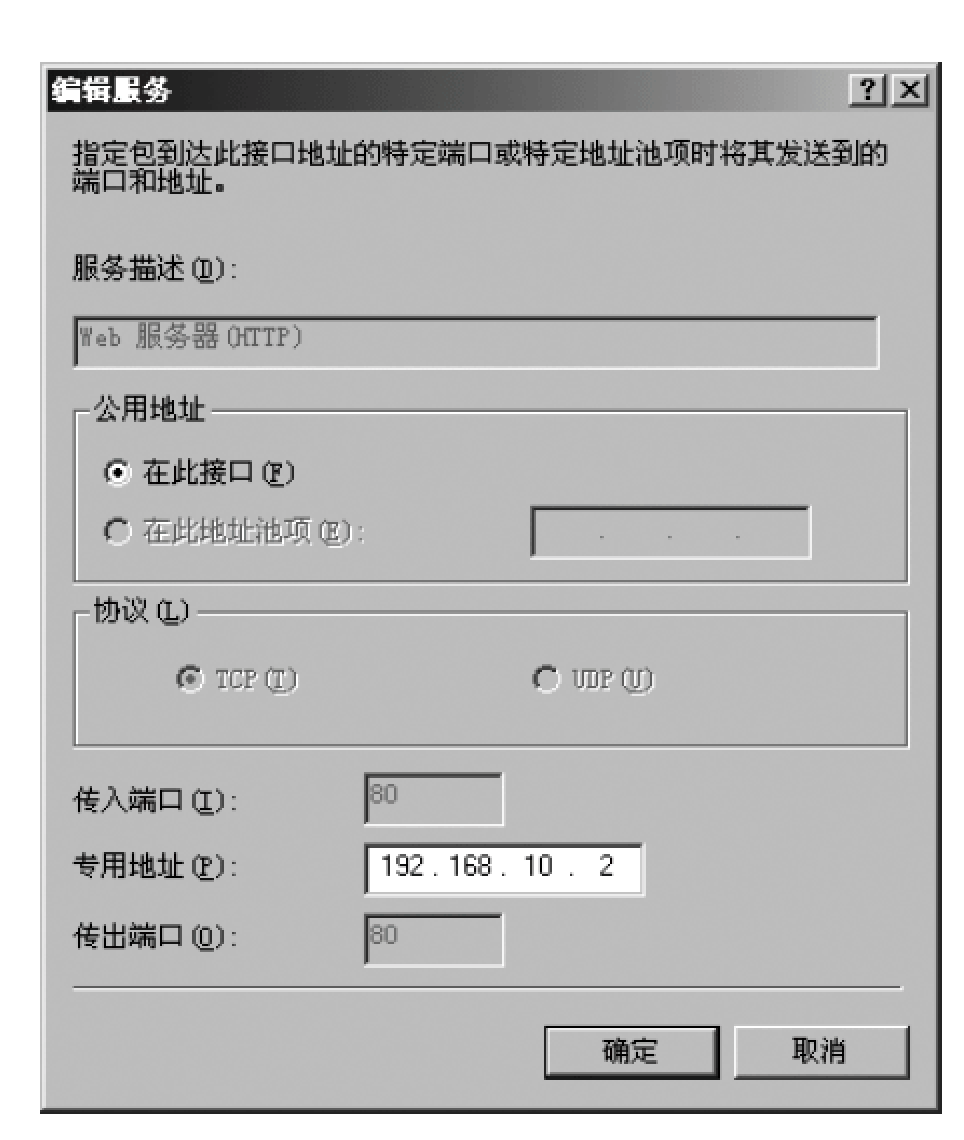


图 11-42 配置端口映射

其中的“公用地址”选择“在此接口”单选按钮，表示由 ISP 分配给 NAT 服务器的公网 IP 地址，“专用地址”是指外部传送给 IP 地址为 59.70.142.248、端口为 80 的 TCP 数据包，NAT 服务器都会将其转换为专用 IP 地址为 192.168.10.2、端口为 80 的服务器软件来负责。

11.7.3 地址映射

通过 TCP/UDP 端口映射技术，开放 NAT 服务器的某些端口，实现外部网络的计算机与内部网络的计算机互相通信。但对某些特殊的应用程序来说，例如某些网络游戏，只开放部分端口是不行的，此时可以通过“地址映射”技术来解决这个问题。只有 NAT 服务器具有多个公共 IP 地址时，才可以使用地址映射。

如果已经申请了多个公共的 IP 地址，则可以把这些公共的 IP 地址添加到 NAT 服务器的地址池内，操作步骤如下。

打开“路由和远程访问”控制台，展开服务器，展开“IP 路由选择”中的“NAT/基本防火墙”，选择连接外部网络的网络接口，右击“属性”，打开连接外部网络接口的属性对话框，打开“地址池”选项卡，如图 11-43 所示。

单击“添加”按钮，然后输入起始和结束的公共 IP 地址，如图 11-44 所示。

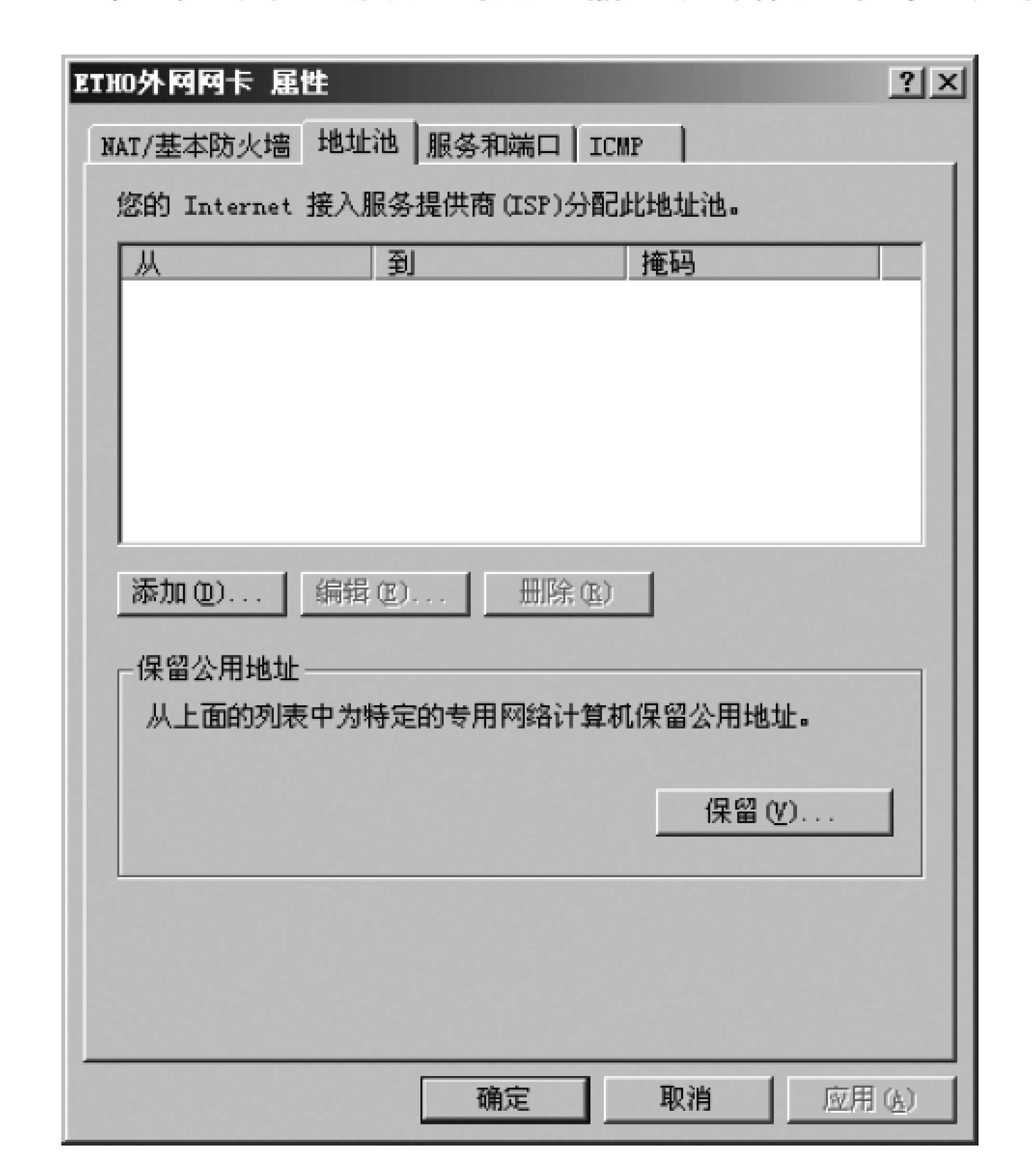


图 11-43　添加地址池

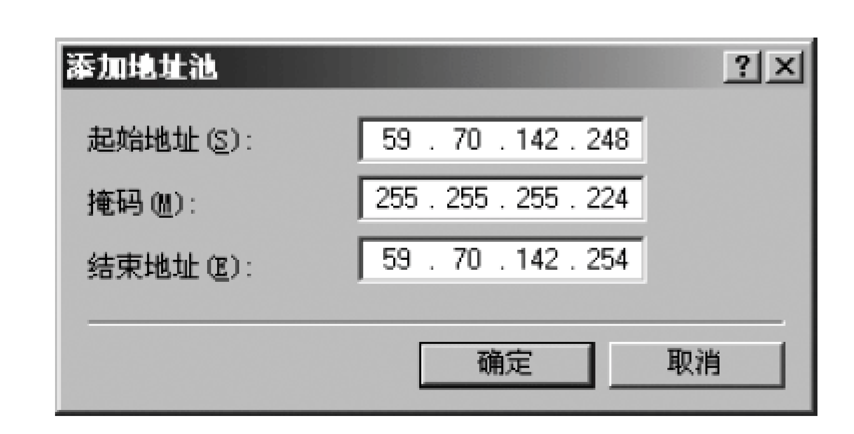


图 11-44　输入起始和结束的公共 IP 地址

单击“确定”按钮，完成向地址池内添加多个公共 IP 地址的操作。

单击“地址池”选项卡中的“保留”按钮，弹出如图 11-45 所示的“地址保留”对话框，可以保留一些公共的 IP 地址与私有 IP 地址进行地址映射。

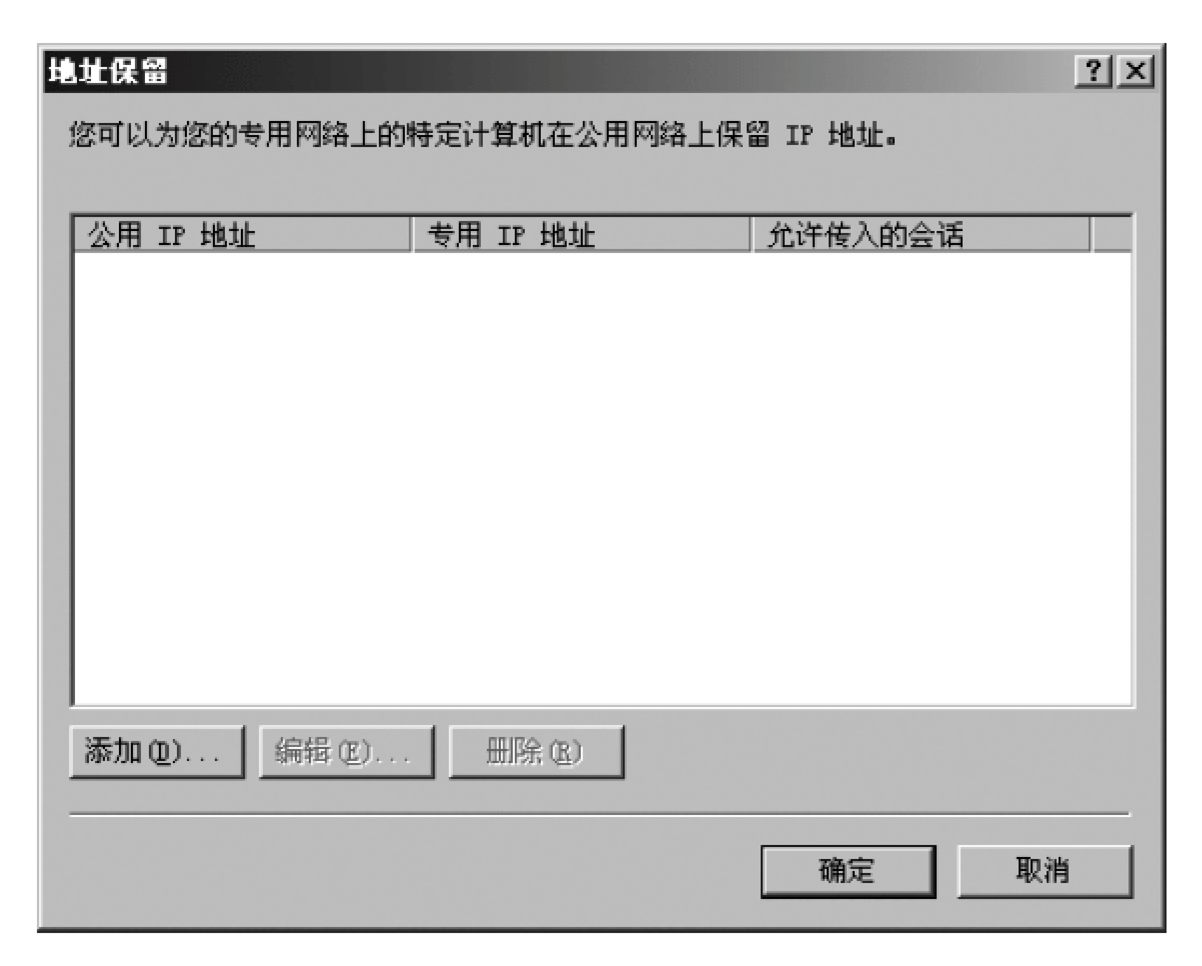


图 11-45　“地址保留”对话框

单击“添加”按钮，弹出如图 11-46 所示的“添加保留区”对话框，可以将地址池中的公有 IP 地址 59.70.142.253 保留给使用私有 IP 地址为 192.168.10.5 的这台计算机。

这样所有从外部传送给 IP 地址为 59.70.142.253 的数据包，都会被 NAT 服务器转发给 IP 地址为 192.168.10.5 的计算机。

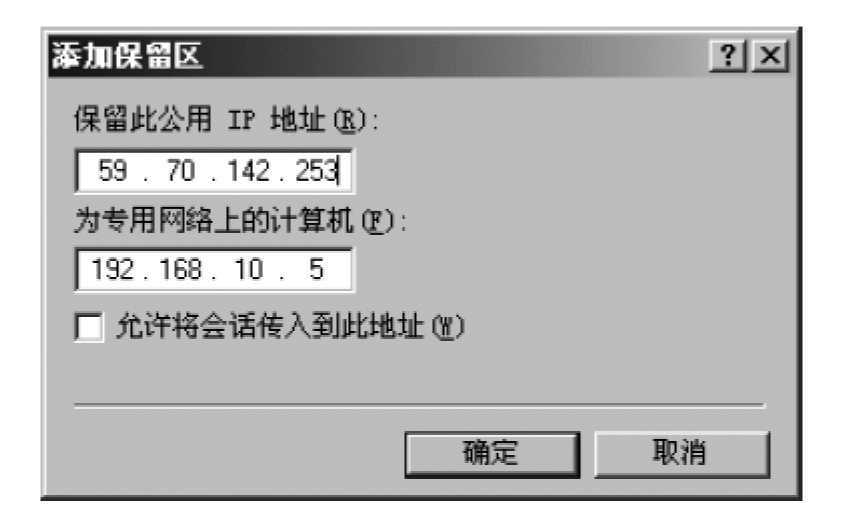


图 11-46 “添加保留区”对话框

从外网传送到内网的各种数据包之中,NAT 服务器默认只接收响应内部计算机请求的数据包,不接收由外部计算机主动与内部计算机通信的数据包。若要让外面的计算机主动与内部计算机通信,则必须选中“允许将会话传送到此地址”复选框,如果这时也没有针对公共 IP/私有 IP 做任何数据包筛选的安全设置,这时就实现了私有 IP 与公有 IP 的一一对应,则内部这台使用私有 IP 的计算机将处于完全开放的状态。

第 12 章　终 端 服 务

学习目标

学习完本章后，了解 Windows Server 2003 终端服务的基本概念，掌握终端服务器安装、配置以及客户端配置的过程，掌握如何在终端服务器上安装应用程序，了解终端服务与远程桌面的区别。

12.1　终端服务概述

Windows Server 2003 通过终端服务（Terminal Services）技术，提供了以下两个功能。

(1) 远程桌面。使用该功能系统管理员可以远程管理计算机，此功能已经内置在 Windows Server 2003 内，无须额外安装，但每一台被管理的计算机最多只允许 2 个人连接。

(2) 多用户同时执行位于终端服务器内的应用程序。将 Windows Server 2003 设置为终端服务器后，可以在这台终端服务器上安装应用程序，并且这些应用程序可以让网络上的多个用户来同时执行。

用户通过远程桌面连接软件连接终端服务器时，必须在终端服务器上或终端服务器所在的域中有合法的用户名和密码，这些用户隶属于 Remote Desktop Users 内置组或系统管理员组。用户连接成功后，就可以执行终端服务器上的应用程序、保存文件、使用网络资源，就像是坐在终端服务器旁边直接操作一样。实际上，客户端计算机的屏幕上只是显示终端服务器上的输出结果，应用程序是在终端服务器上执行，在客户端计算机上只是利用键盘、鼠标执行输入动作。每个用户连接到终端服务器后只能看到自己的会话，该会话独立于其他客户端的会话。通过终端服务器上多会话环境的设置，多个远程用户可以同时访问终端服务器的桌面或应用程序。

安装终端服务器后，虽然可以供多人同时执行位于终端服务器内的应用程序，但是只有 120 天的使用期限，120 天后终端服务器会拒绝用户的连接，除非网络中有一台已经被激活的终端服务器，并且取得合法的授权连接数量。也就是说 120 天后，用户必须经过“终端服务器授权服务器”的授权后，才可以连接终端服务器。可以利用安装“终端服务器授权”服务来建立“终端服务器授权服务器”。

12.2　安装与配置终端服务器

如果只是想使用 Windows Server 2003 提供的远程桌面管理功能，并且不超过 2 个用户连接，这时就不需要安装终端服务，Windows Server 2003 默认情况下已经安装了远

程桌面管理组件。但如果要允许多个用户同时执行服务器上的应用程序，就必须安装终端服务。

12.2.1　安装终端服务器

在 Windows Server 2003 计算机上，安装终端服务的操作步骤如下。

(1) 单击“开始”→“控制面板”→“添加或删除程序”→“添加/删除 Windows 组件向导”，在“Windows 组件向导”对话框中选中“终端服务器”前的复选框，如图 12-1 所示，单击“下一步”按钮。

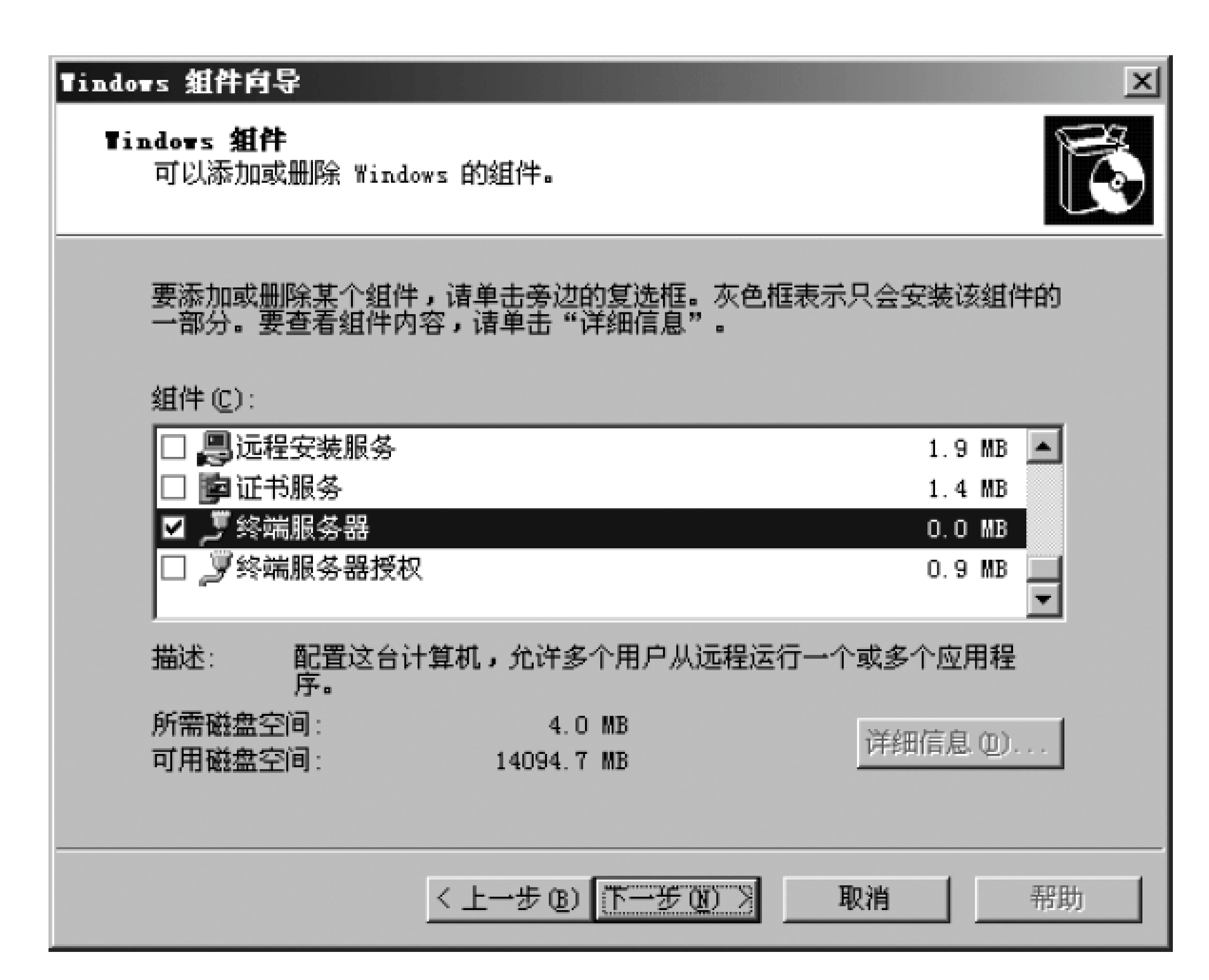


图 12-1　“Windows 组件向导”对话框

(2) 出现图 12-2，提示有关安装终端组件的信息，单击“下一步”按钮。

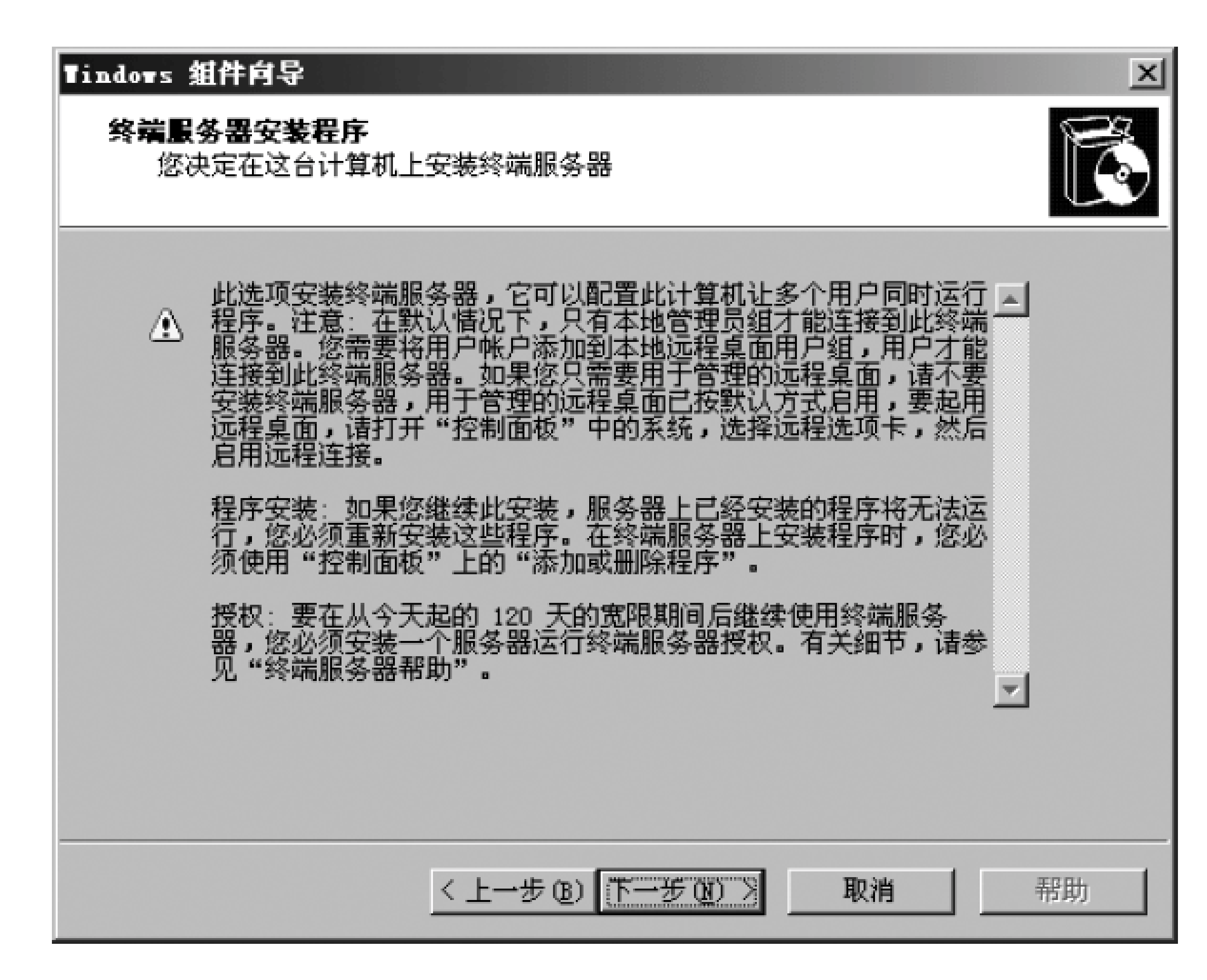


图 12-2　提示有关安装终端组件的信息框

（3）在图12-3中，有两种选择：完整安全模式和宽松安全模式。具体使用哪种安全模式需要根据实际需求，在此选择默认值“完整安全模式”，单击“下一步”按钮。

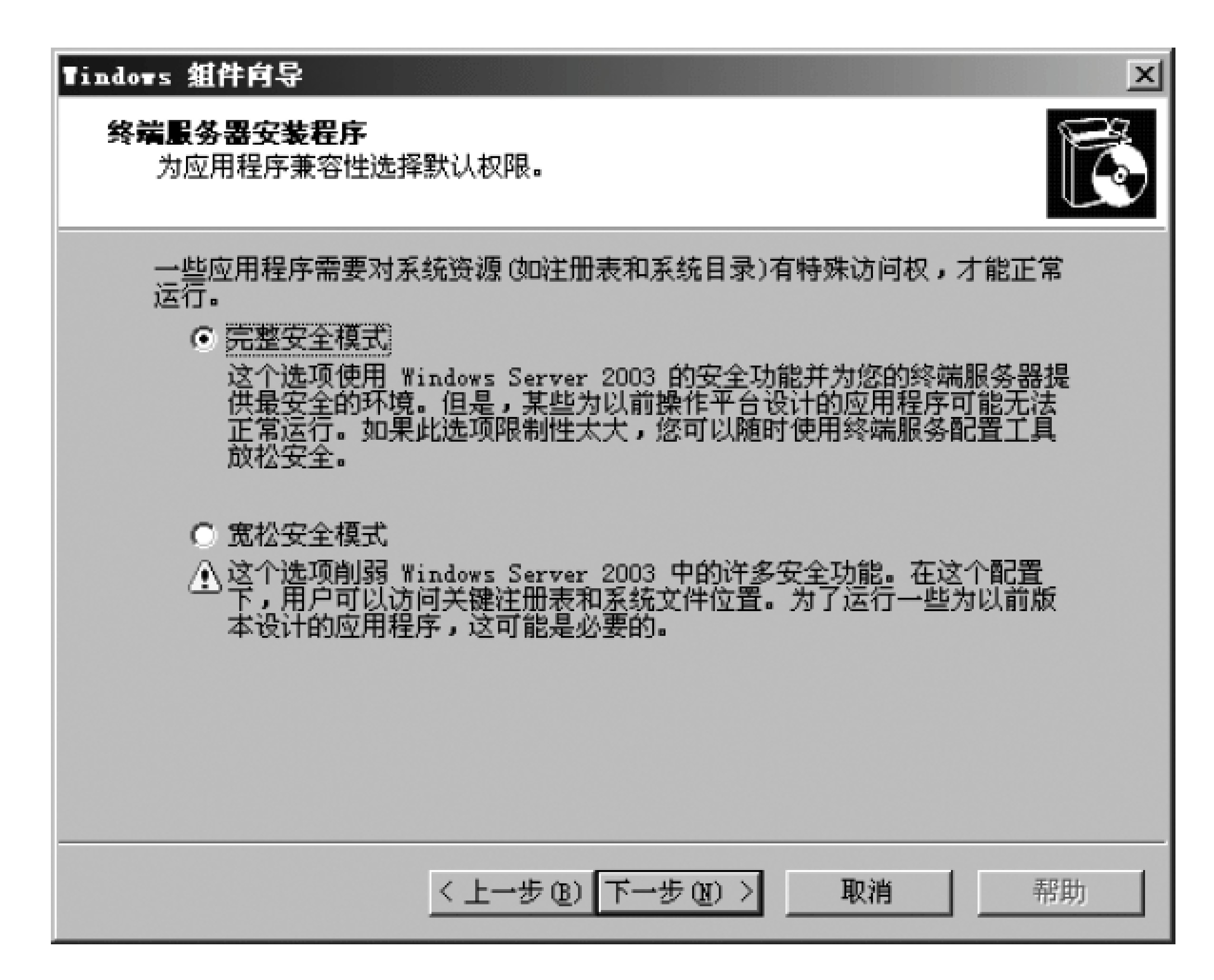


图12-3 为应用程序兼容性选择默认权限

（4）在图12-4中，有3种终端许可方式。

① 使用下列许可证服务器。公司的网络一般都没有专门的许可证服务器。

② 使用自动搜索的许可证服务器。将自动搜索网络中的许可证服务器，适合许可证服务器不固定的网络使用。

③ 我将在120天内指定许可证服务器。先使用终端服务120天，之后再购买许可证，建立相应的许可证服务器。

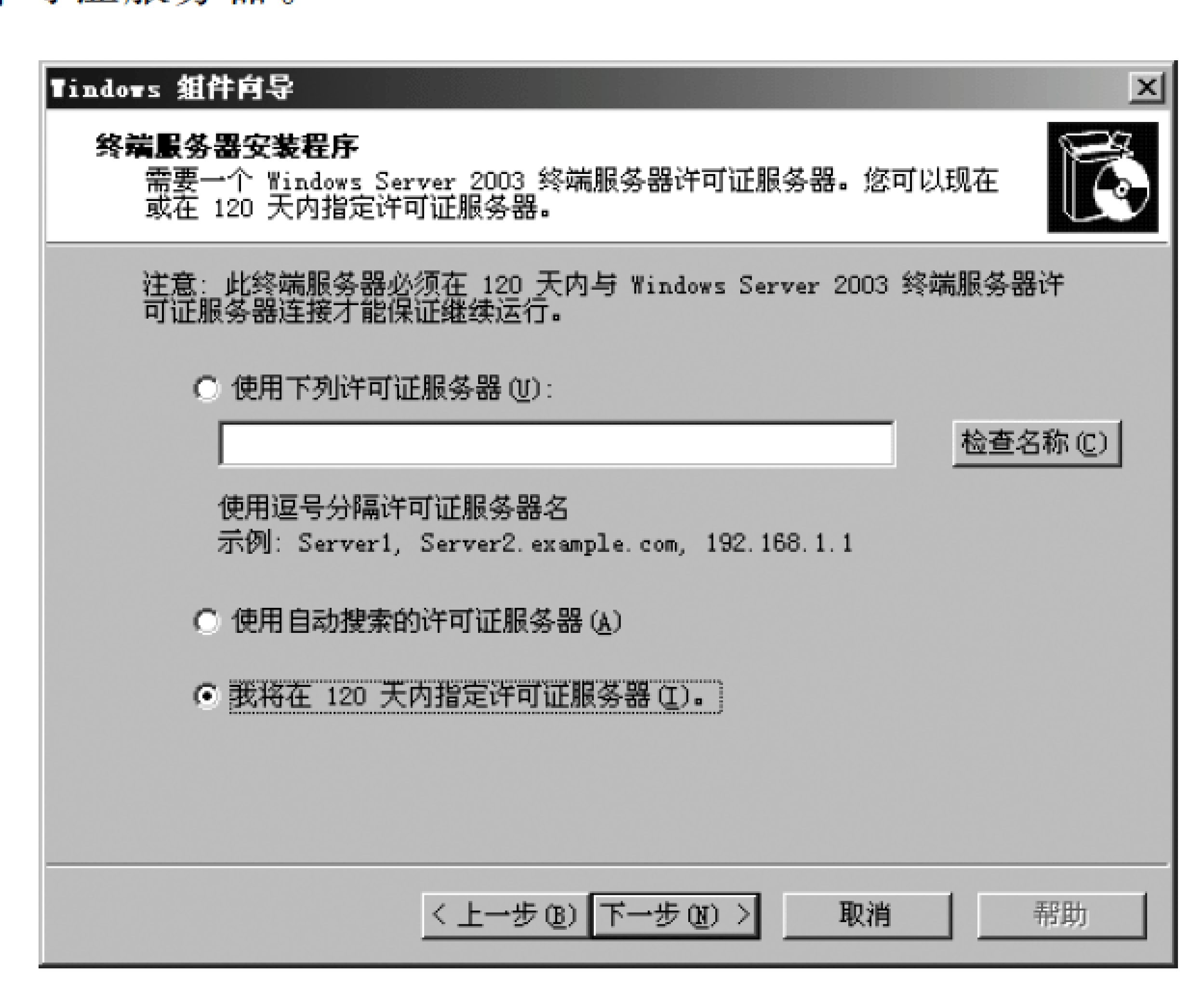


图12-4 指定许可证服务器

具体使用哪种许可方式，要根据实际情况选择，这里选择“我将在120天内指定许可

证服务器”单选按钮，单击“下一步”按钮。

(5) 出现图 12-5 所示的授权模式，有两种选择。

① 每设备授权模式。一个设备一个授权，只能在具有授权许可证的设备上使用终端服务。

② 每用户授权模式。一个用户一个授权，只有经过授权的用户才能使用终端服务。

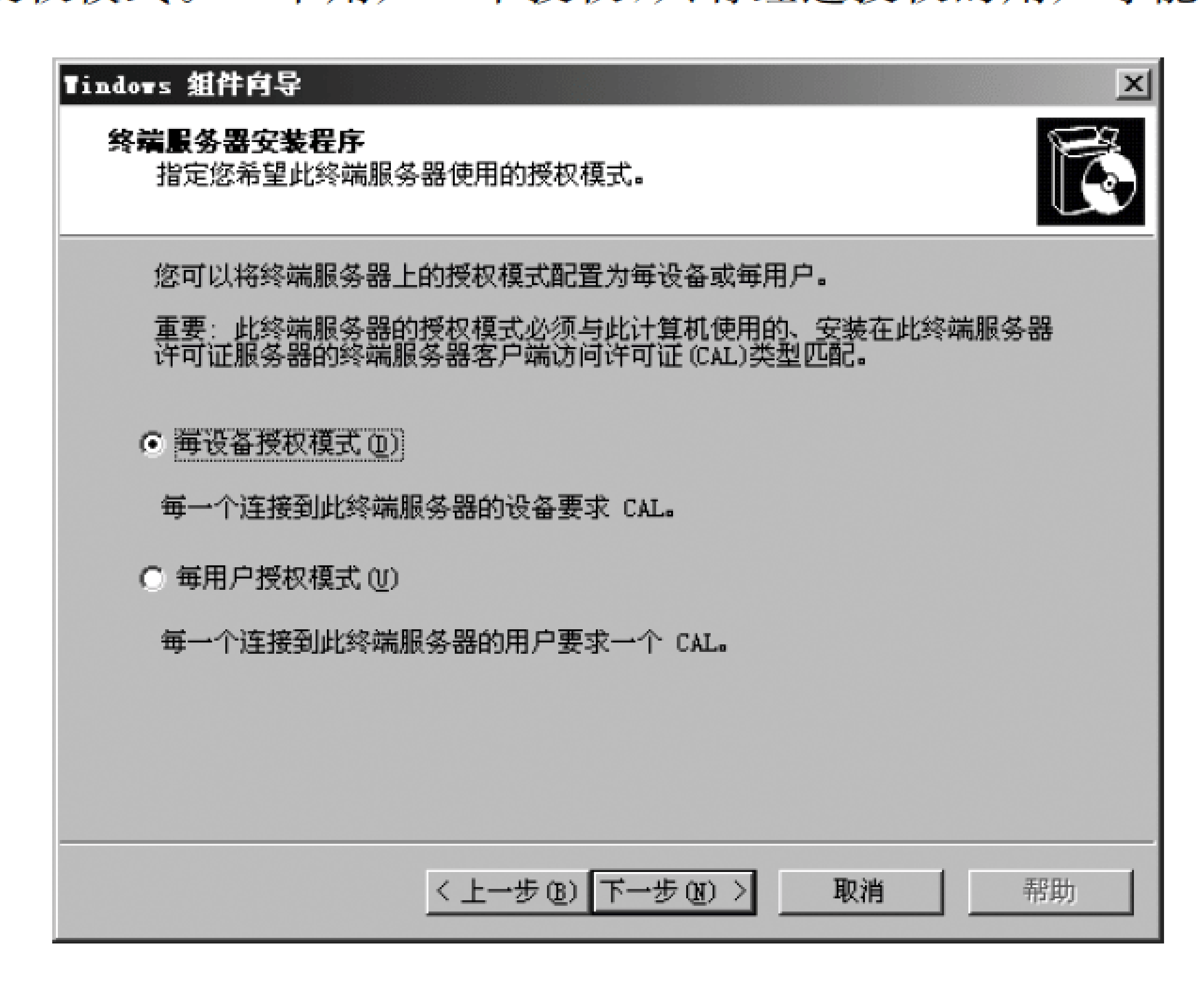


图 12-5　指定授权模式

在向微软公司购买授权许可证前，这些选项都是没有意义的。具体使用哪种授权模式，管理员要根据实际情况做出选择，这里选择“每设备授权模式”单选按钮，单击“下一步”按钮。

(6) 出现安装进度画面，当出现“完成 Windows 组件向导”时，单击“完成”按钮重新启动系统，即可完成终端服务器的安装。

12.2.2　客户端所需软件

Windows Server 2003、Windows XP 客户端计算机已经内置了“远程桌面连接”客户端软件，无须额外安装就可以连接到终端服务器。而 Windows Server 2000、Windows NT 等客户端计算机必须单独安装这些客户端软件。“远程桌面连接”安装软件位于终端服务器的%systemroot%\system32\clients\tsclient\win32 文件夹内，可以将此文件夹设为共享文件夹，然后让用户连接到此共享文件夹，并执行其中的安装程序 SETUP.EXE。安装完成后，可以通过单击“开始”→“程序”→“附件”→“通信”→“远程桌面连接”的方式来连接终端服务器。

12.2.3　授予用户通过终端服务登录的权限

为使用户能登录到终端服务器，必须在提供终端服务的计算机上开启“远程桌面”，并

且要将用户账户加入到 Remote Desktop Users 组,用户才可以利用“远程桌面连接”来连接到终端服务器或远程计算机。将用户加入到 Remote Desktop Users 组的方式,与这台提供终端服务的计算机是否安装终端服务器有关。

1. 未安装终端服务器时

如果未安装终端服务器,只提供远程桌面管理的功能,则授予用户能够连接到这台计算机的远程桌面的操作步骤如下。

(1) 单击“开始”→“控制面板”→“系统”→“远程”选项卡,出现图 12-6,提示用于远程桌面连接的账户必须有密码,并且防火墙需要打开相应的端口才能正常访问,单击“确定”按钮。

(2) 出现图 12-7,选择“远程”选项卡,选中“启用这台计算机上的远程桌面”前的复选框,即可启动远程桌面连接。

图 12-6 提示用于远程桌面连接的账户必须有密码

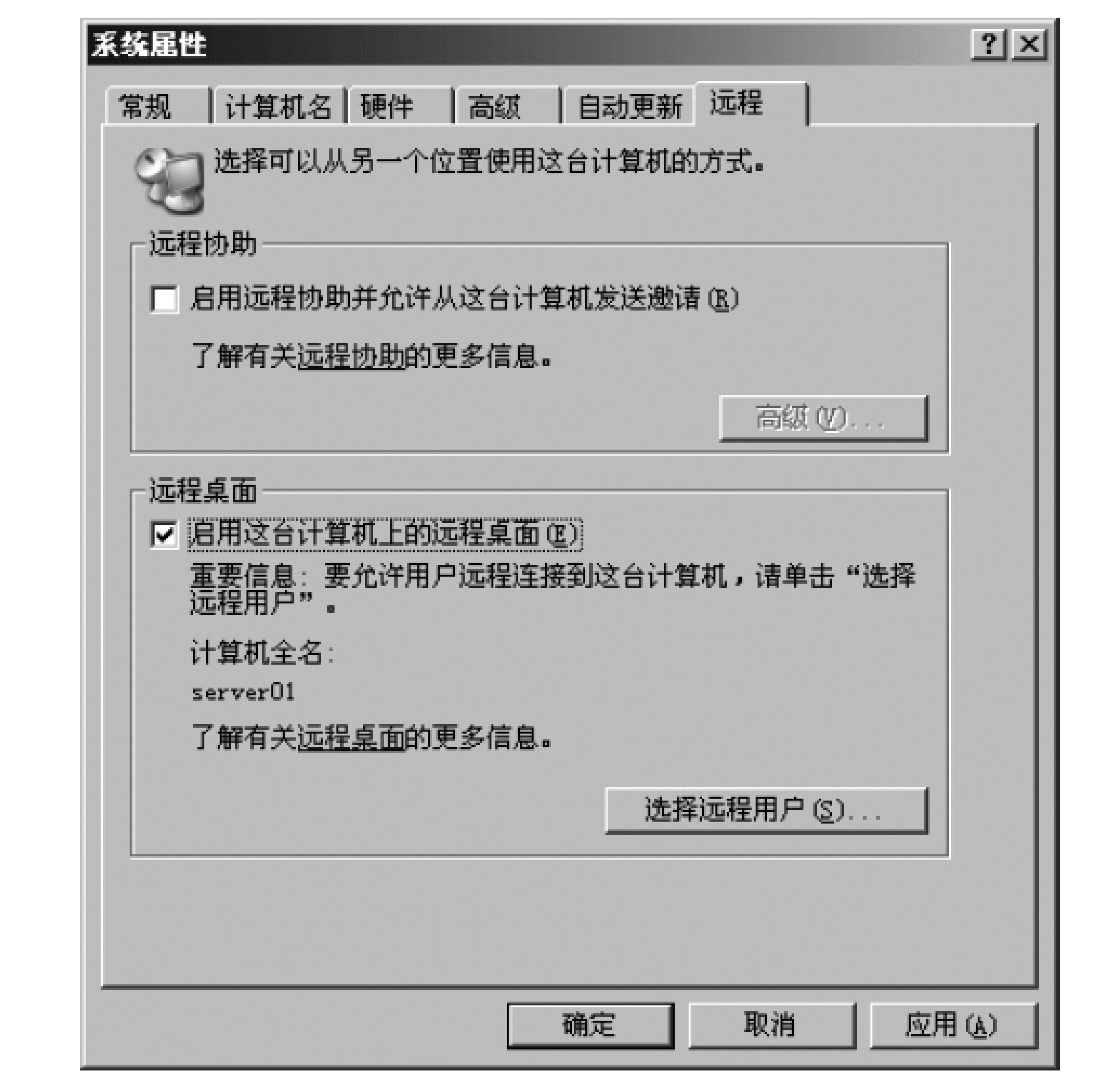


图 12-7 启用这台计算机上的远程桌面

(3) 单击图 12-7 中的“选择远程用户”按钮,出现图 12-8。单击“添加”按钮,将用户加入到 Remote Desktop Users 组。

默认情况下,Administrator 账户已经具有远程桌面访问权限。新建的其他用户需要加入到 Remote Desktop Users 组或管理员组后才能进行远程桌面访问。

2. 安装了终端服务器时

如果已经安装了终端服务器,授予用户终端服务访问权限的操作步骤如下。

(1) 单击“开始”→“控制面板”→“系统”→“远程”选项卡,选取“启用这台计算机上的远程桌面”复选框即可,如图 12-9 所示。

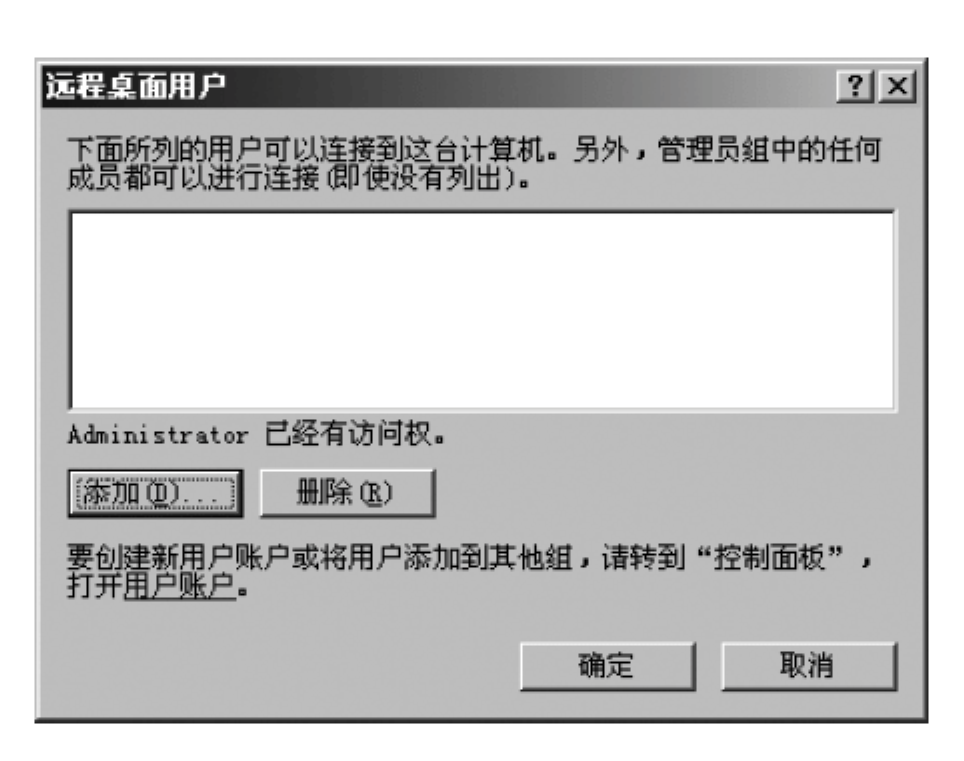


图 12-8　添加远程桌面用户

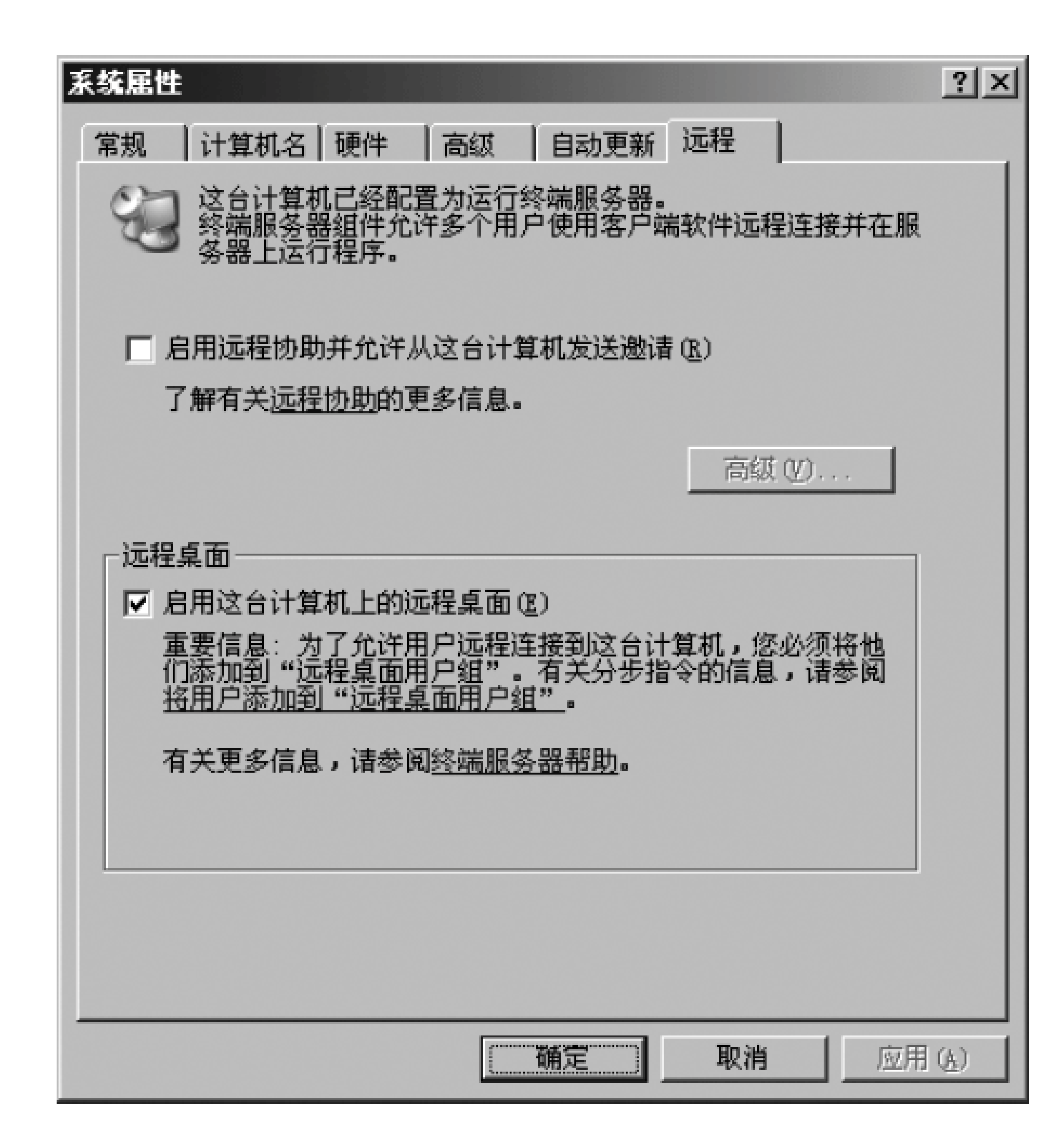


图 12-9　启用计算机上的远程桌面

(2) 如果此计算机是域控制器，请打开“Active Directory 用户和计算机”管理工具，将用户加入 Remote Desktop Users 组，该组位于 Builtin 容器内，如图 12-10 所示。

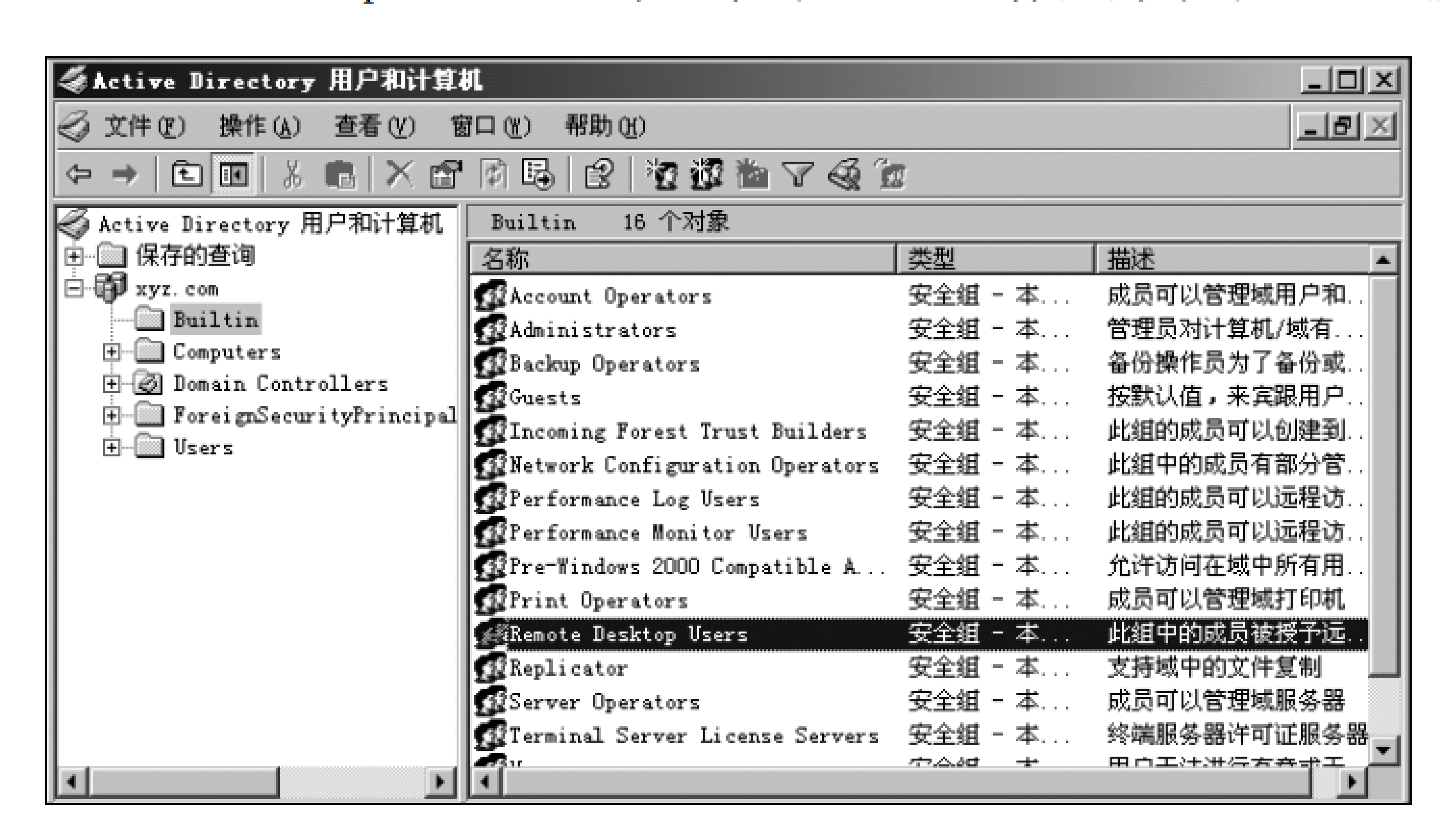


图 12-10　Remote Desktop Users 组

(3) 如果是成员服务器、独立服务器，单击“开始”→“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”，将用户加入 Remote Desktop Users 组，如图 12-11 所示。

3. 在组策略中修改通过终端服务允许登录的权限

默认情况下，Windows Server 2003 成员服务器、独立服务器与 Windows XP 计算机内的 Remote Desktop Users 组已经具备了“允许通过终端服务登录”的权限。但在域控制器上，Remote Desktop Users 组却没有这个权限，授予该权限的操作步骤如下。

(1) 在域控制器上，单击“开始”→“管理工具”→“域控制器安全策略”→“安全设

置”→“本地策略”→“用户权限分配”,如图 12-12 所示。

图 12-11　将用户加入 Remote Desktop Users 组

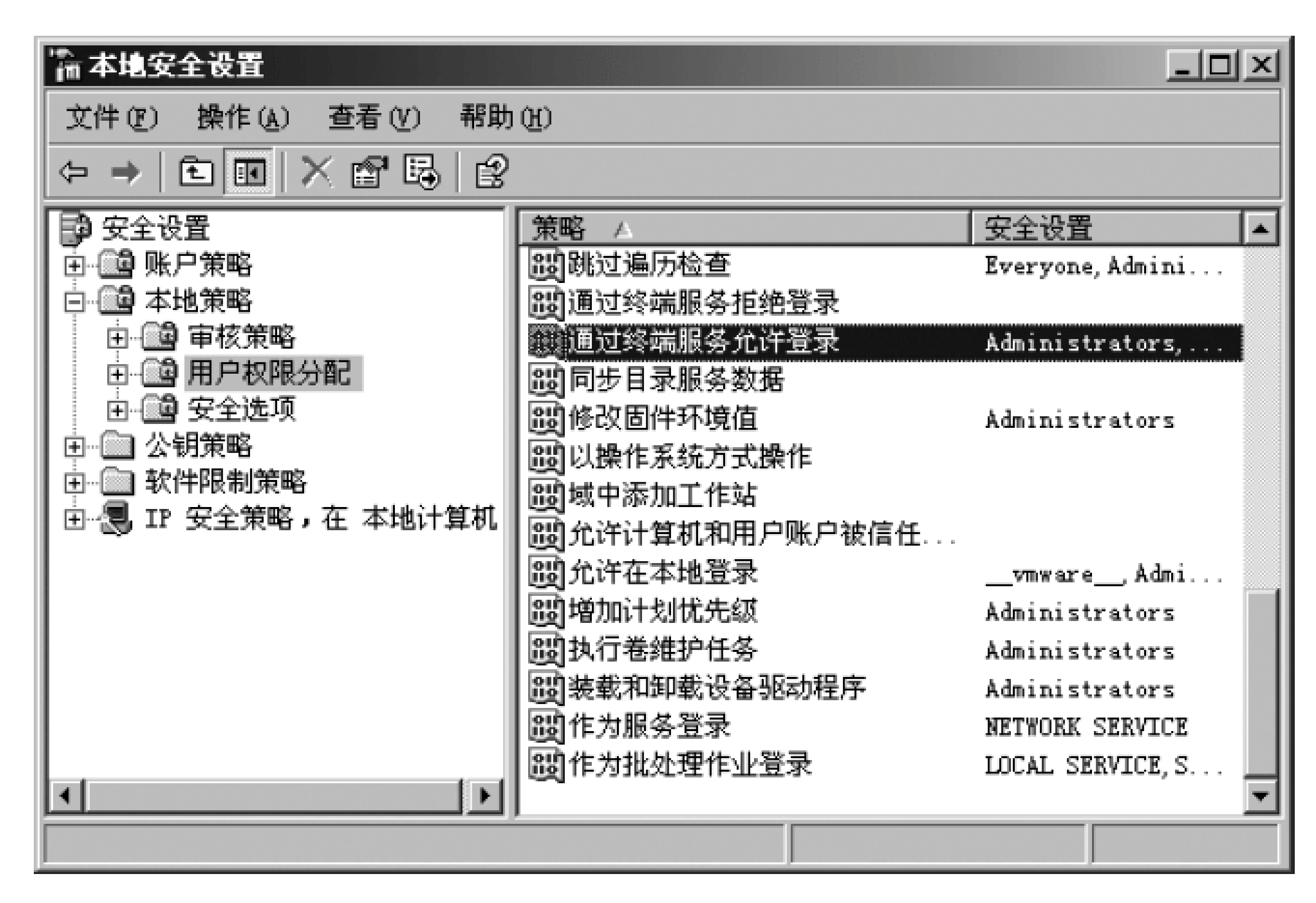


图 12-12　通过终端服务允许登录策略

(2) 双击“通过终端服务允许登录”策略,添加 Remote Desktop Users 组,如图 12-13 所示。

(3) 单击“确定”按钮,即可完成该策略项的设置,系统默认 5min 后应用此策略到域控制器,重新开机也会应用,也可以在命令提示符下执行 gpupdate/target:computer/force 命令强制刷新以应用组策略。

12.2.4　如何连接到终端服务器

在 Windows Server 2003 计算机上,要利用“远程桌面连接”连接到终端服务器,操作步骤如下。

(1) 单击“开始”→“程序”→“附件”→“通信”→“远程桌面连接”,在图 12-14 中,输入需要连接的终端服务器或远程计算机的 IP 地址或计算机名称或完整的主机名称。



图 12-13　设置通过终端服务允许登录策略



图 12-14　远程桌面连接

(2) 当出现图 12-15 所示的界面时，输入用于登录的用户名和密码后，单击“确定”按钮。



图 12-15　输入用于登录的用户名和密码

(3) 若出现图 12-16 所示的登录消息警告框，则表示可能是该用户未加入 Remote Desktop Users 组，或是输入的用户名和密码错误。

(4) 登录成功后，可以看到终端服务器或远程计算机的桌面。

用户完成在终端服务器上的操作任务后，需要注销或断开与终端服务器的连接。

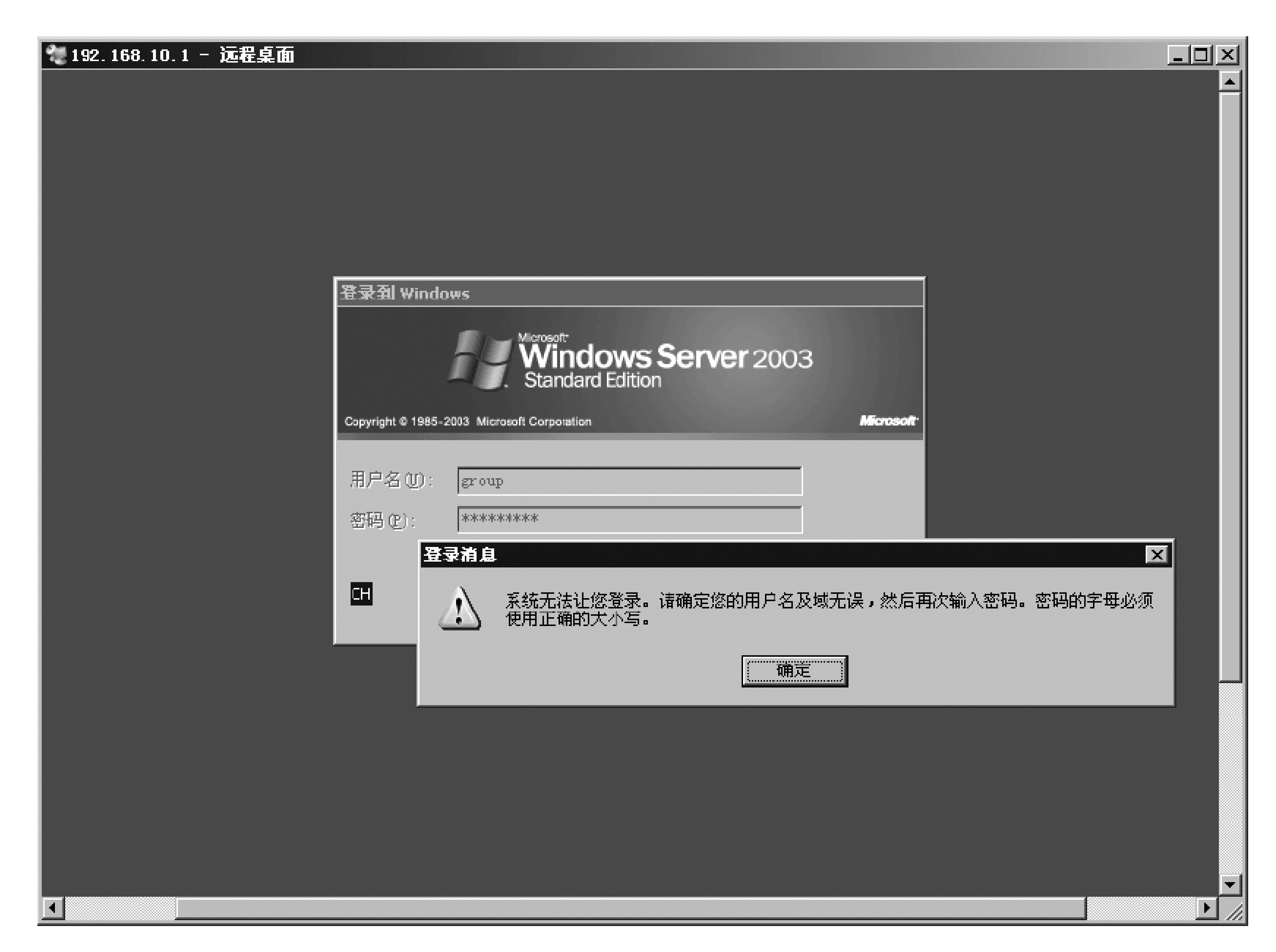


图 12-16　建立远程桌面连接时输入的用户名和密码错误

① 在远程桌面窗口中，单击“开始”→“注销”，或使用 Ctrl＋Alt＋End 组合键即可注销与终端服务器的连接，注销后，用户在终端服务器上执行的程序会结束。

② 用户可以直接单击远程桌面窗口右上方的×，即关闭按钮来断开与终端服务器的连接，断开连接并不会结束用户正在终端服务器上运行的程序，并且这些程序会在终端服务器上继续运行，用户下一次即使是从另外一台计算机上来重新连接终端服务器，也会继续先前打开的会话。

12.3　配置终端服务器

要更改终端服务器的设置，操作步骤如下。

在终端服务器上，单击“开始”→“程序”→“管理工具”→“终端服务配置”，打开如图 12-17 所示的对话框，右击 RDP-Tcp，可以更改终端服务的设置，如图 12-18 所示。



图 12-17　更改终端服务的设置

1. 登录设置

选择“登录设置”选项卡，可以设置用户登录终端服务器的方式，如图 12-19 所示。

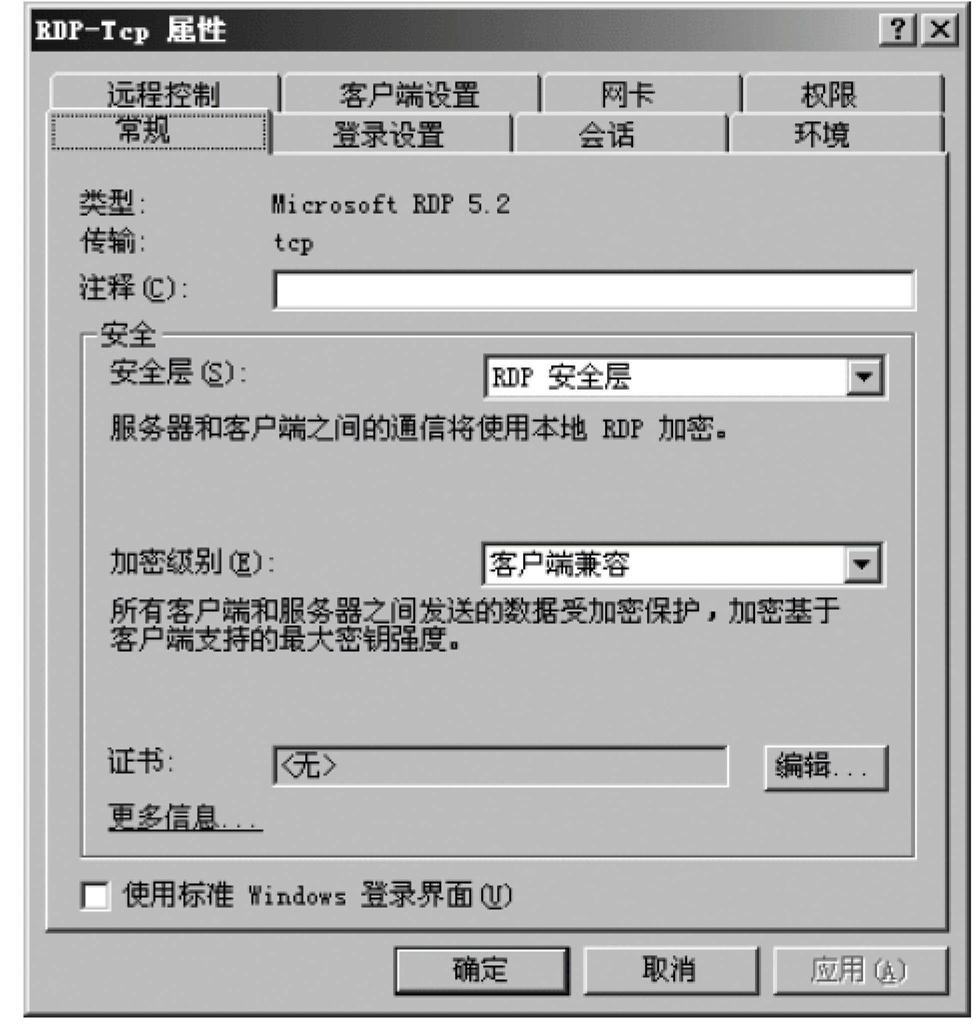


图 12-18 终端服务的常规设置



图 12-19 终端服务的登录设置

(1) 使用客户端提供的登录信息。客户端在登录终端服务器时，终端服务器利用客户端提供的用户名和密码进行验证。

(2) 总是使用下列登录信息。指定一个固定的用户名、密码，让所有连接到终端服务器的用户都自动利用这个账户登录。但这样可能会引发安全问题，一般不建议使用。

(3) 总是密码提示。不论用户的远程桌面连接软件是否指定了用户名和密码来自动连接，每次连接时都会要求用户输入用户名和密码。

2. 远程控制设置

选择“远程控制”选项卡，可以设置该计算机被远程控制的方式，如图 12-20 所示。

远程控制允许从一个会话远程控制另一个用户的会话，用于监视或随时控制另一个登录到终端服务器的会话。假设有一个连接到终端服务器的用户在执行终端服务器内的应用程序时，不知道该如何操作，可以利用终端服务器所提供的远程控制功能，以系统管理员的身份取得他的远程桌面连接控制权，以指导该用户如何操作应用程序。

(1) 使用具有默认用户设置的远程控制。表示用户能否被远程控制由用户账户的属性决定。打开“Active Directory 用户和计算机”或“本地用户和组”来检查设置。以域用户账户为例，其远程控制属性如图 12-21 所示，选取“启用远程控制”复选框，可使该用户被远程控制。

(2) 不允许远程控制。该用户与终端服务器之间的会话，无法被远程控制。

(3) 使用具有下列设置的远程控制。所有用户的会话都可以被控制，并且可以决定如何被远程控制。

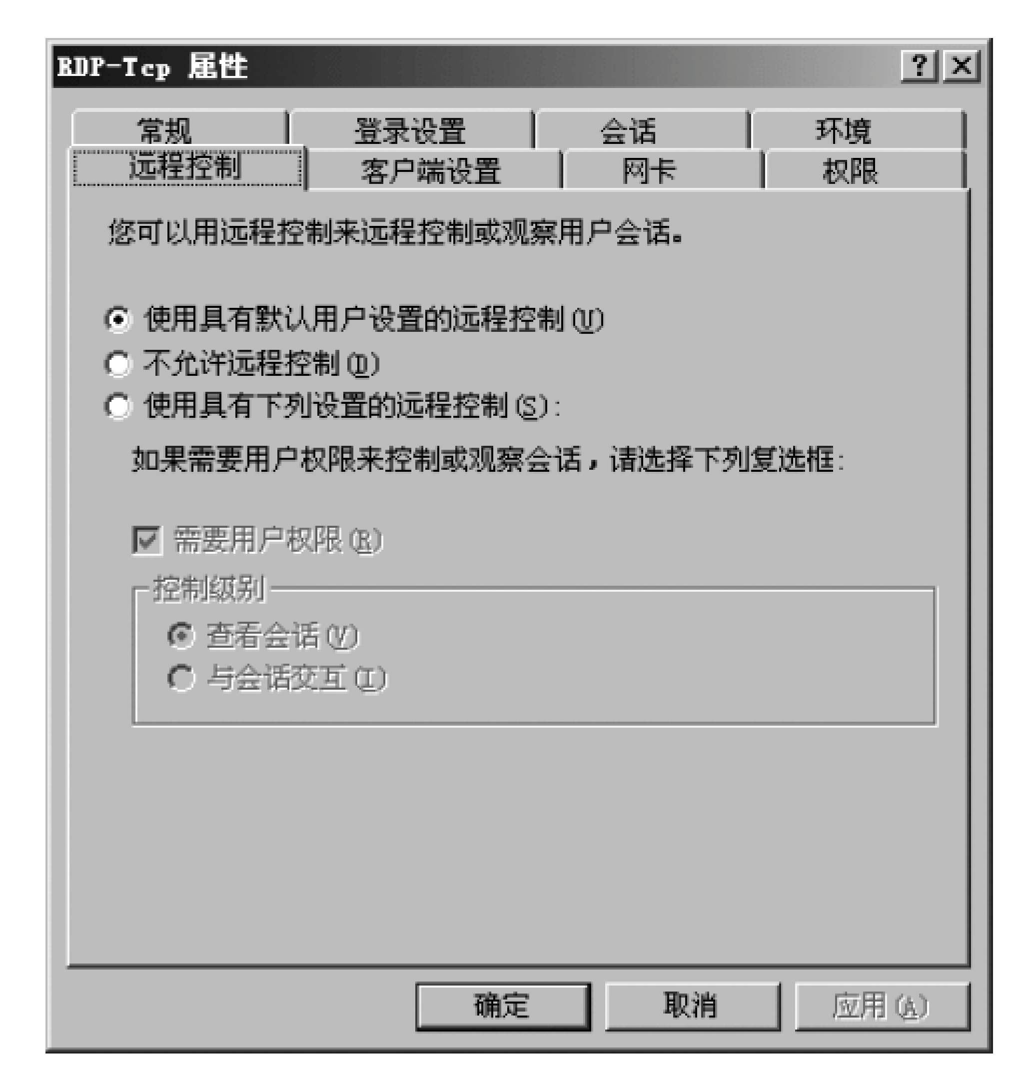


图 12-20 终端服务的远程控制设置

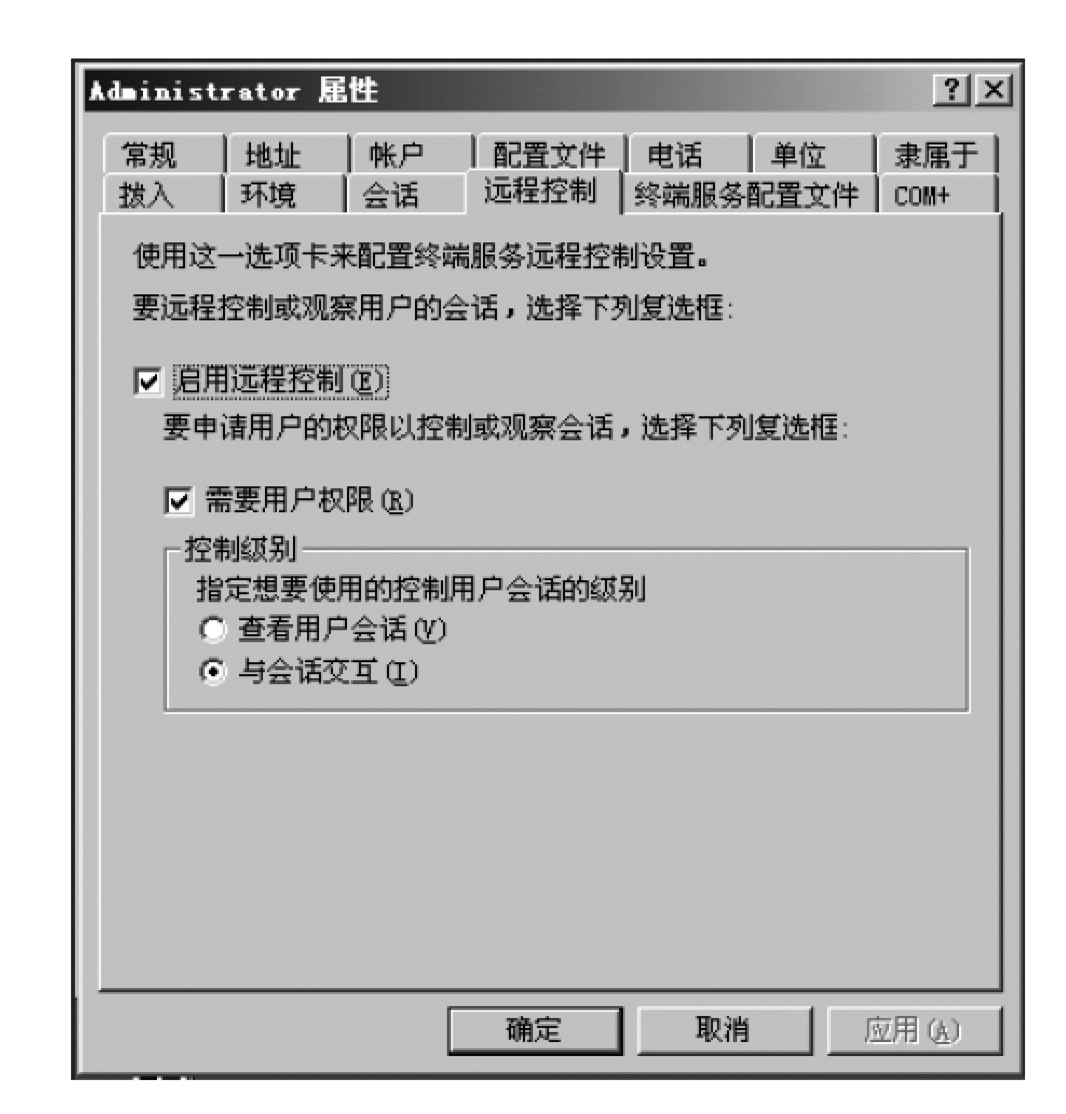


图 12-21 启用远程控制

① 需要用户权限。当用户被远程控制时，要经过该用户的同意。

② 查看会话。只能够查看用户与终端服务器之间的会话。

③ 与会话交互。可以利用键盘、鼠标来操作、控制远程用户与服务器之间的会话。

3. 客户端设置

选择“客户端设置”选项卡，可以配置登录后是否使用客户端的驱动器、打印机等设备，还可以设置颜色深度以及禁用一些项目等，如图 12-22 所示。



图 12-22 终端服务的客户端设置

可以启动或禁用一些本地资源项目的映射功能。

(1) 驱动器映射。设置在远程桌面窗口是否可以使用客户端的本地磁盘驱动器。

(2) Windows 打印机映射。设置在远程桌面窗口是否可以使用客户端的本地打印机。

(3) LPT 端口映射。设置在远程桌面窗口是否可以使用客户端的本地 LPT 端口。若启用该映射,用户在远程桌面窗口添加打印机时,就可以选择本地的 LPT 端口,因此终端服务器内的文件也可以通过连接在本地 LPT 端口的打印机来打印。

(4) COM 端口映射。设置在远程桌面窗口是否可以使用客户端的本地 COM 端口。若启用该映射,用户在远程桌面窗口内使用串口时,也可以选择本地的 COM 端口。

(5) 剪贴板映射。允许在本地与终端服务器之间使用"复制"与"粘贴"命令。

(6) 音频映射。允许终端服务器所发出的声音通过客户端的本地计算机来发声。

4. 终端服务配置文件

要配置终端服务配置文件,操作步骤如下。

单击"开始"→"管理工具"→"Active Directory 用户和计算机",选取用户账户所在的容器,右击用户账户,打开账户属性对话框,单击"终端服务配置文件"选项卡,如图 12-23 所示。

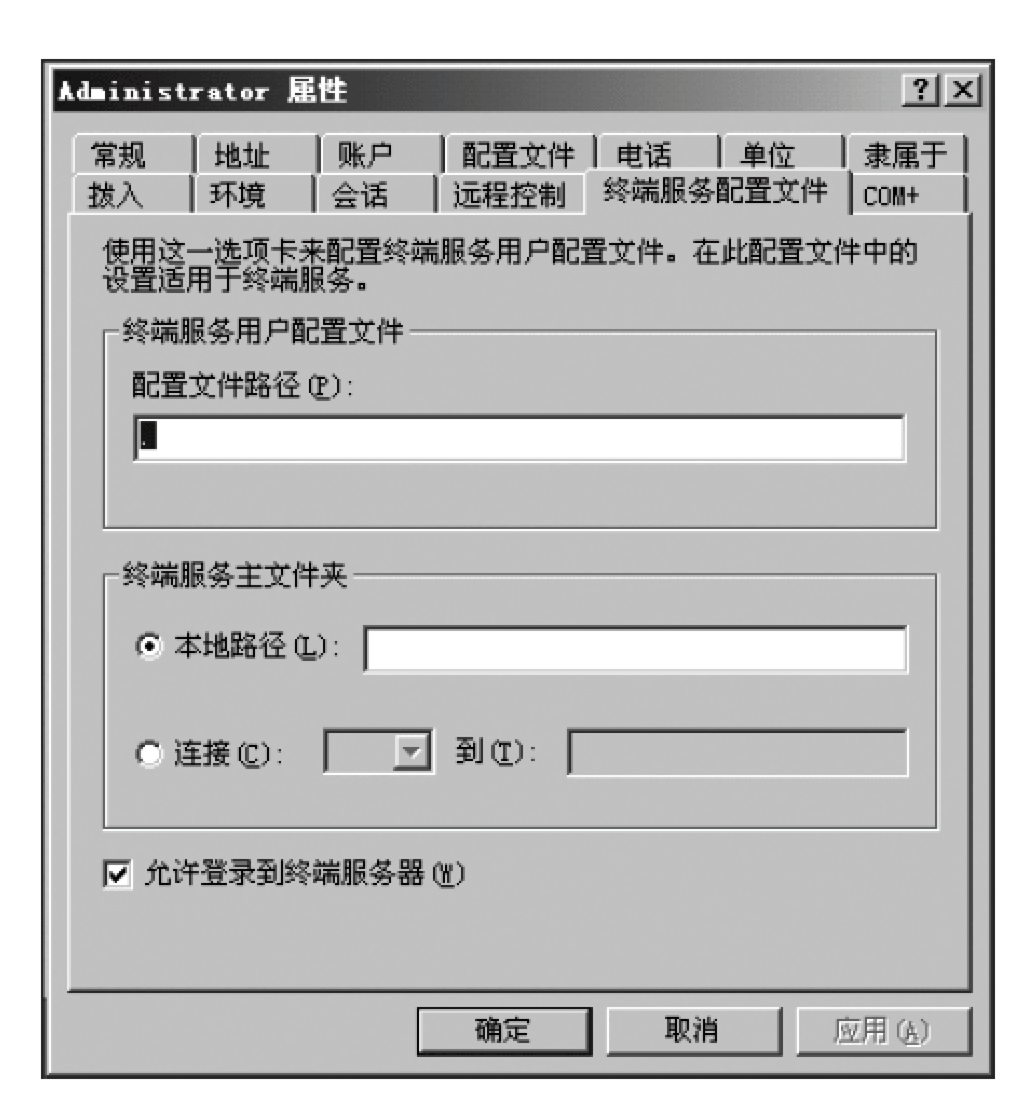


图 12-23 "终端服务配置文件"选项卡

(1) 在"配置文件路径"文本框中输入终端服务配置文件的路径。

(2) 在"终端服务主文件夹"的"本地路径"处,可以指定用于终端服务会话的主文件夹的本地路径,也可以通过"连接"设置终端服务主文件夹的 UNC 路径。

(3) 允许登录到终端服务器。如果禁用此项,则不允许用户登录到任何终端服务器。

12.4 设置客户端的远程桌面连接

在客户端计算机上，要更改远程桌面连接设置，操作步骤如下。

单击“开始”→“所有程序”→“附件”→“通信”→“远程桌面连接”，打开“远程桌面连接”对话框，如图 12-24 所示。



图 12-24 “远程桌面连接”对话框

1. 常规设置

单击图 12-24 中的“选项”按钮，选择“常规”选项卡，如图 12-25 所示。

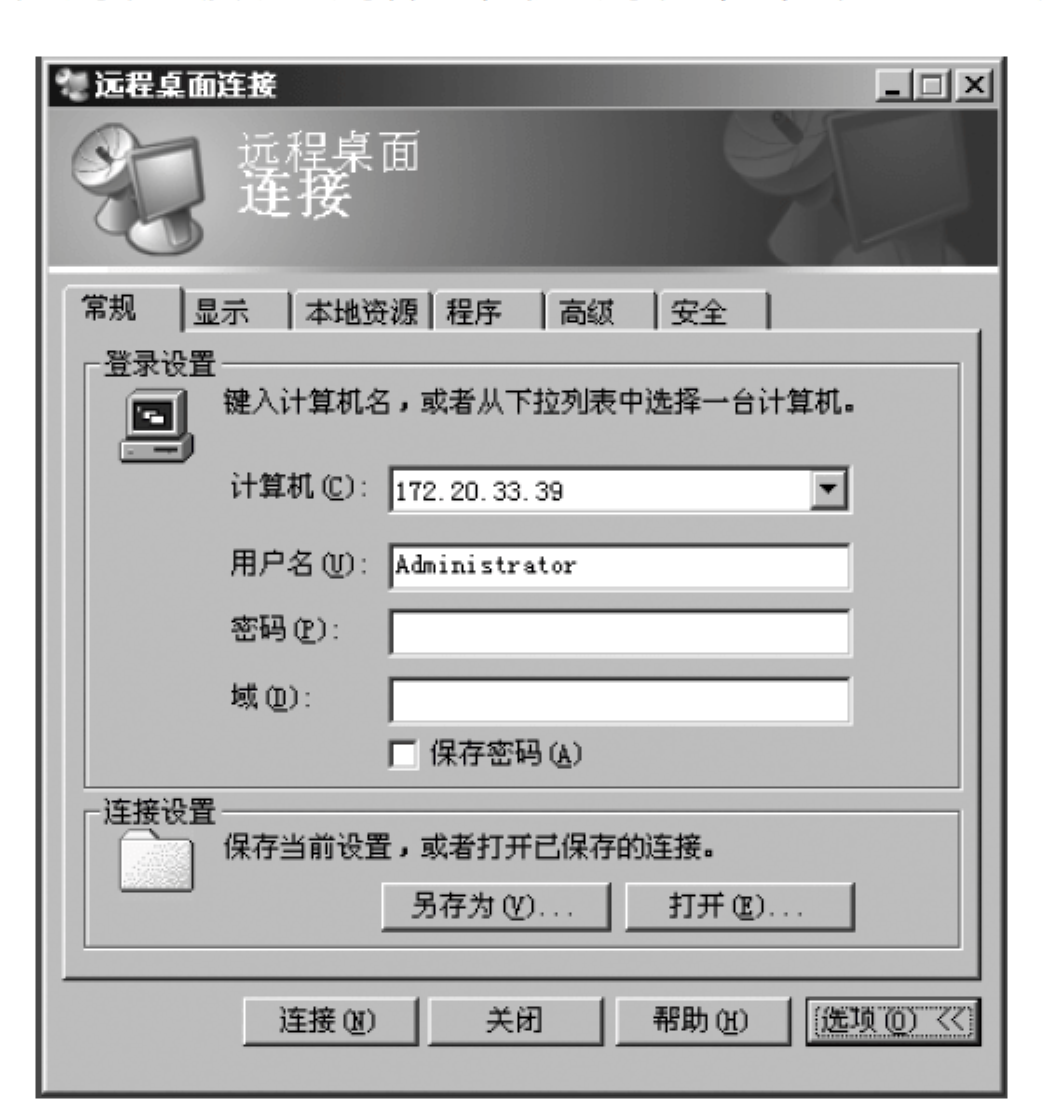


图 12-25 远程桌面连接的“常规”选项卡

在“登录设置”区域的“计算机”文本框中输入要进行远程桌面连接的计算机名称或 IP 地址，在“用户名”文本框中输入用户名，在“密码”文本框中输入用户的登录密码，在“域”文本框中输入要登录的域名称，用户若要保存密码，可选中“保存密码”复选框。在“连接设置”区域单击“另存为”按钮，可将当前的设置信息保存下来，以后用户可直接单击“打开”按钮，打开以前保存的设置。单击“连接”按钮，即可进行远程桌面连接。

2. 显示设置

选择“显示”选项卡,用户可以更改远程桌面的大小和颜色,如图 12-26 所示。

3. 本地资源

选择“本地资源”选项卡,如图 12-27 所示。可以设置远程计算机声音、键盘操作是否带到本地计算机上,以及登录到远程计算机时是否可以使用本地的磁盘驱动器、打印机等设备。

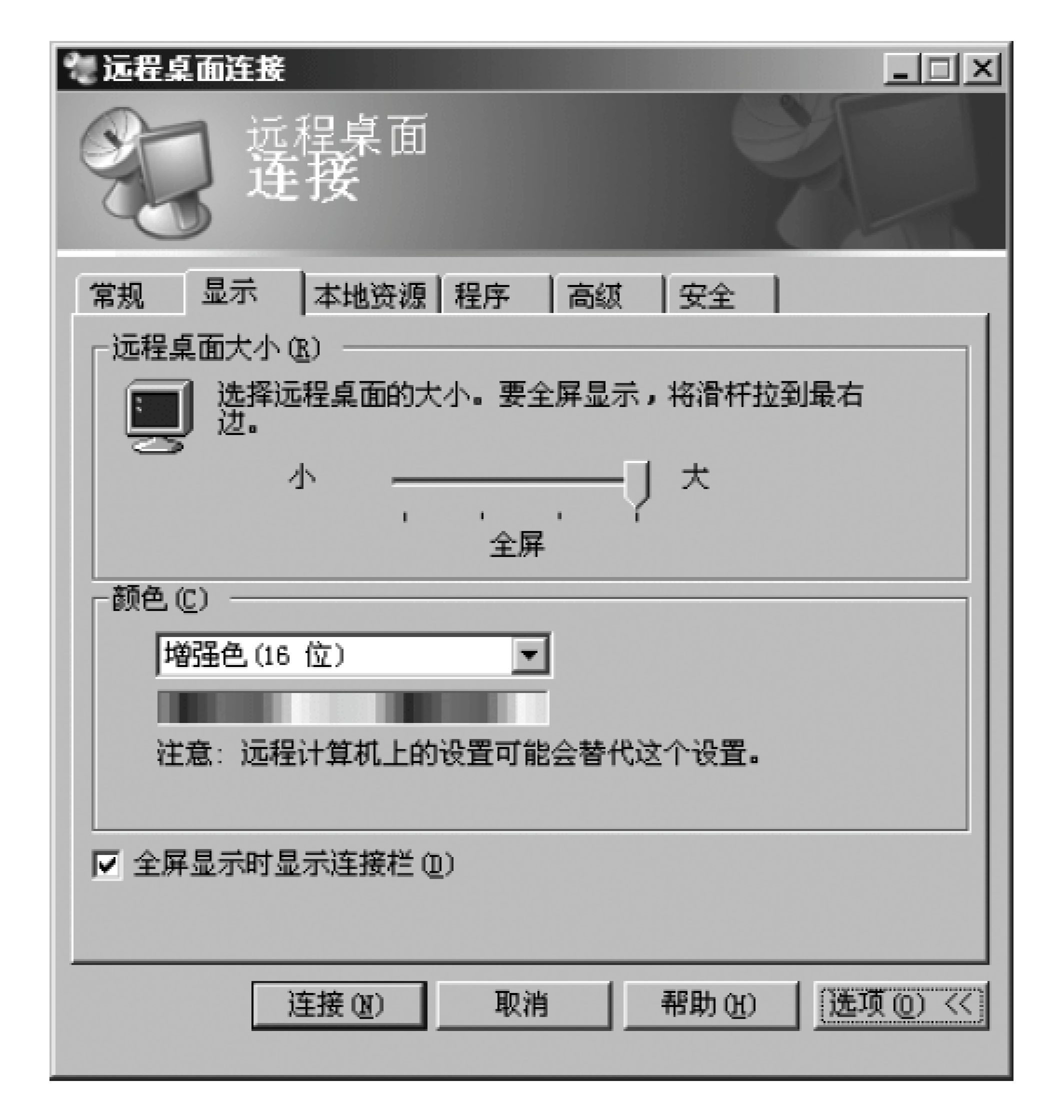


图 12-26　远程桌面连接的“显示”选项卡

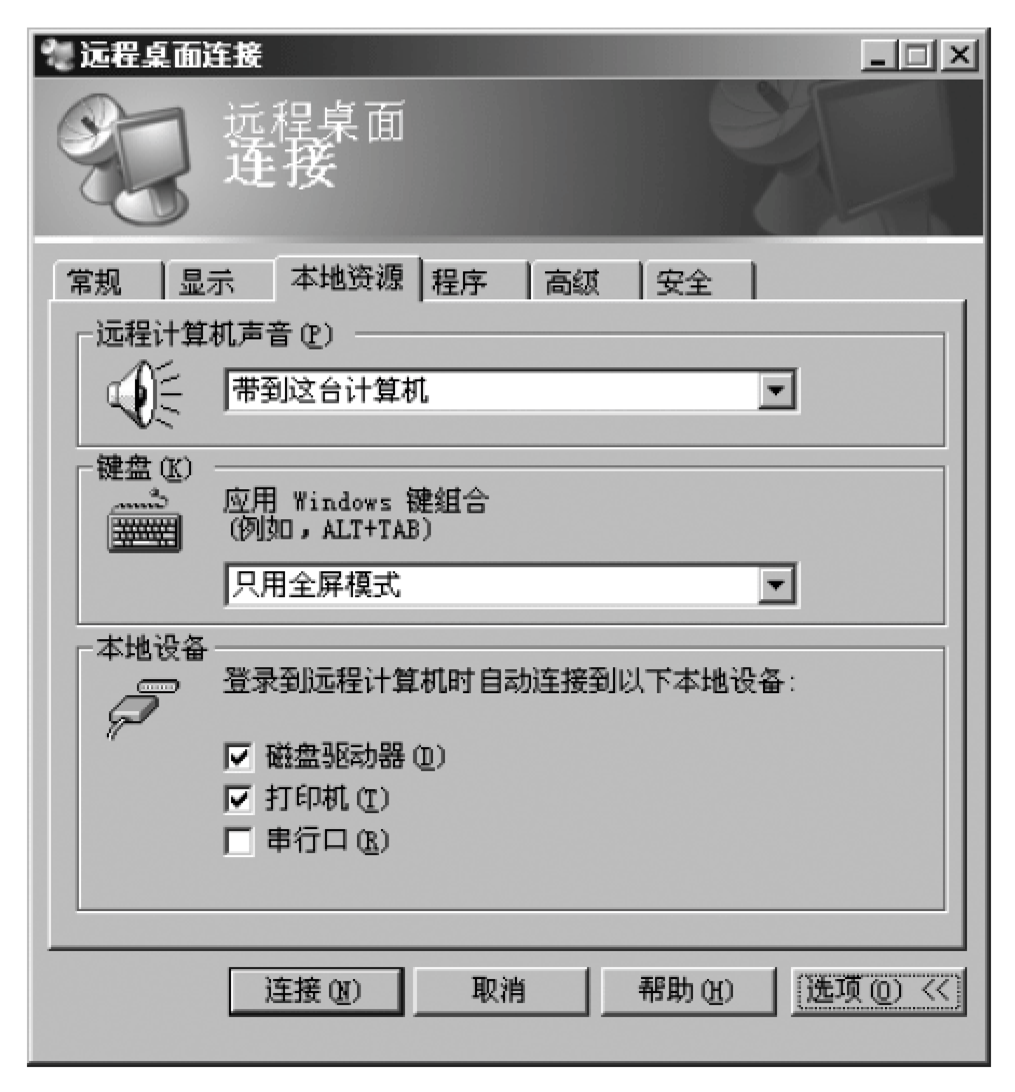


图 12-27　远程桌面连接的“本地资源”选项卡

(1) 远程计算机声音。可设置远程计算机上的声音是带到本地计算机上播放,还是不播放远程计算机上的声音,还是将远程计算机上的声音留在远程计算机上。

(2) 键盘。当用户应用 Windows 组合键时,设置用来操作的是本地计算机,还是远程计算机,还是只在全屏模式下才操作远程计算机。

(3) 本地设备。设置用户在登录到远程计算机时是否自动连接磁盘驱动器、打印机及串口等本地设备。例如,若选中“磁盘驱动器”复选框,成功建立远程桌面连接后,允许在远程计算机与本地计算机之间进行文件的移动、复制、粘贴等操作。

4. 程序

选择“程序”选项卡,如图 12-28 所示,可以设置在连接时自动启动指定的程序。

5. 高级设置

选择“高级”选项卡,如图 12-29 所示,可以根据本地计算机与远程计算机之间连接的速度来调整、优化远程桌面连接的设置。在条件允许的情况下,尽可能选择较高的连接速

度，以使其发挥更大的性能。

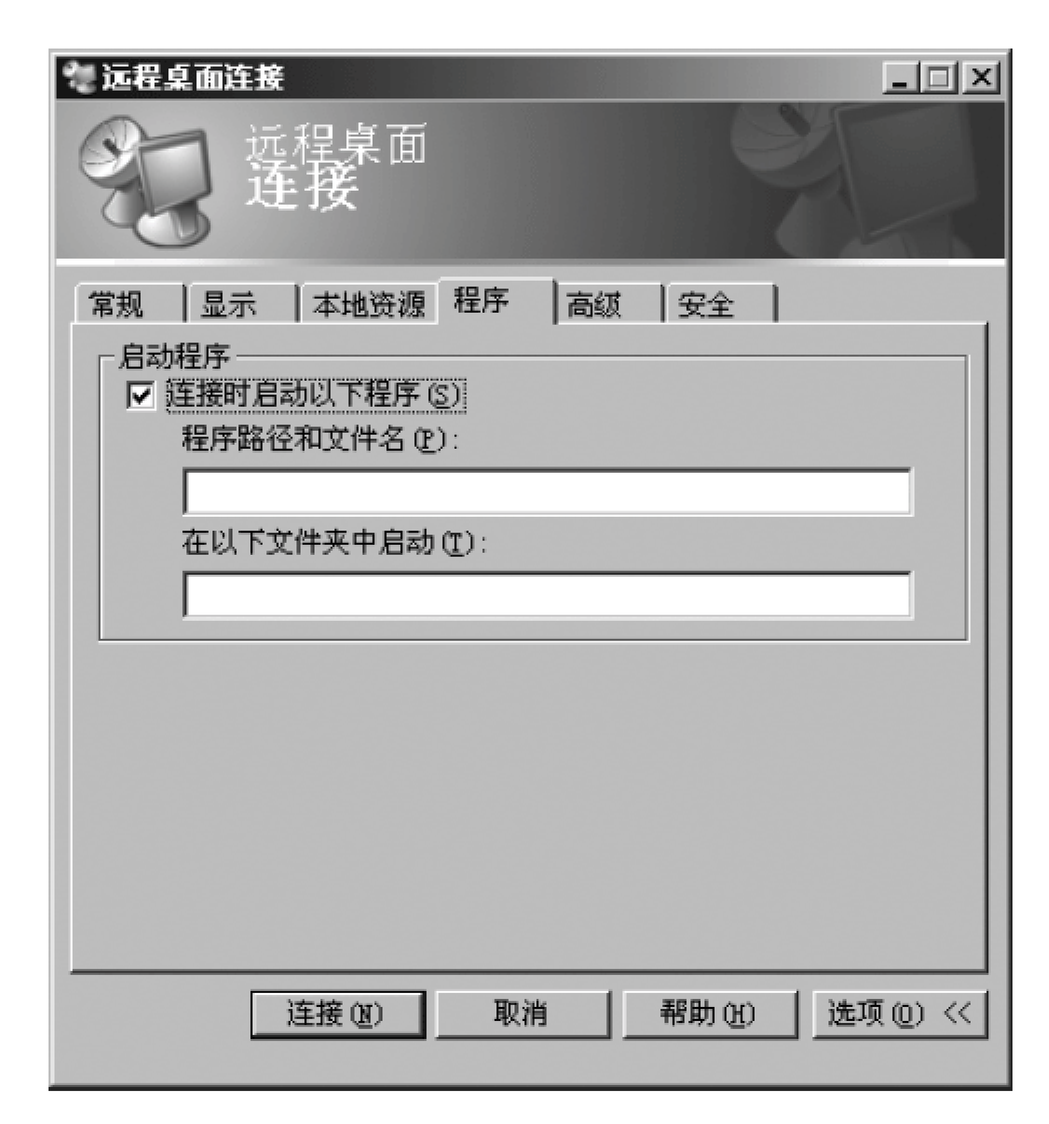


图 12-28 远程桌面连接的“程序”选项卡

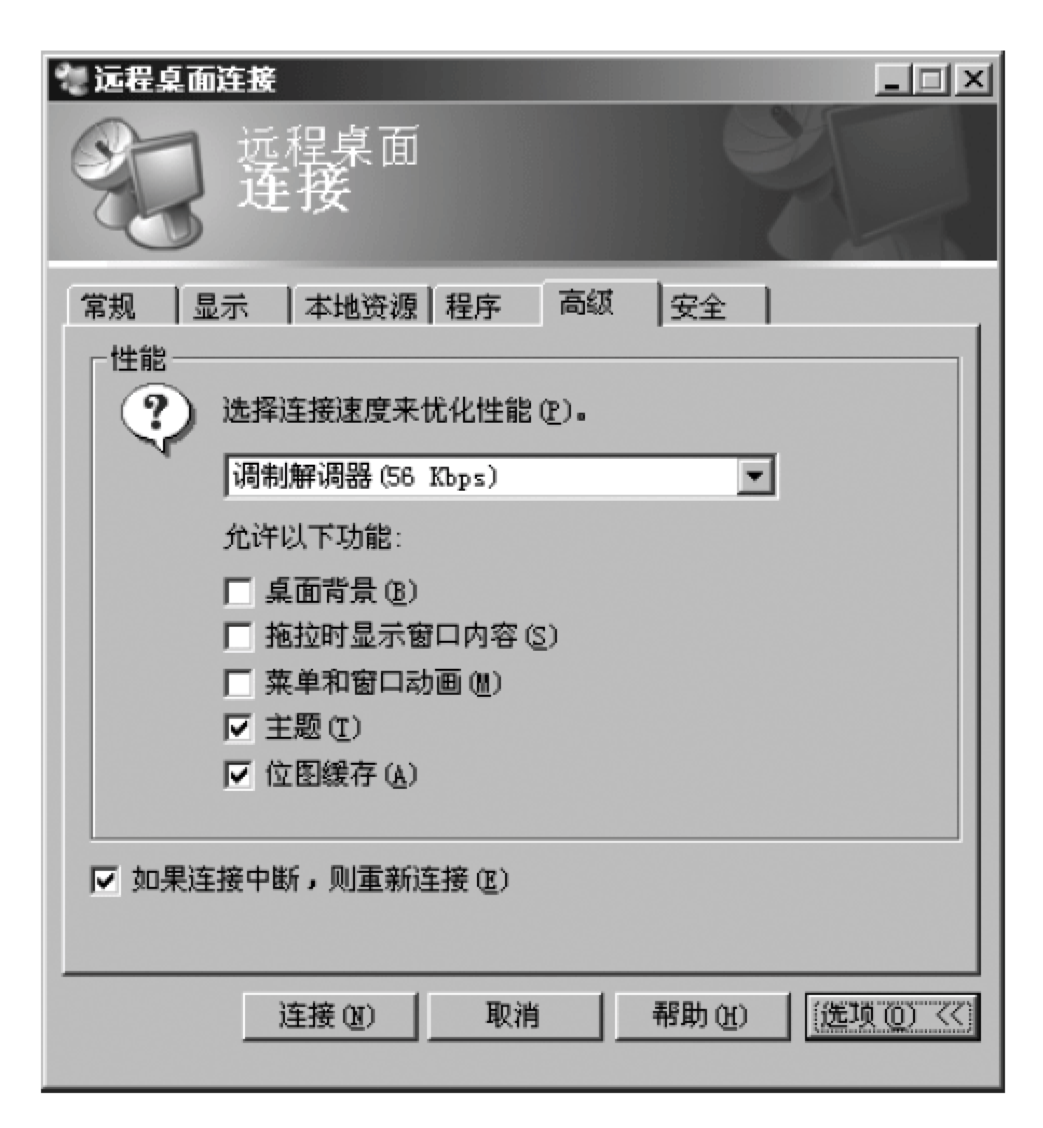


图 12-29 远程桌面连接的“高级”选项卡

12.5 终端服务和远程桌面的区别

终端服务仅仅存在于 Windows Server 2000 和 Windows Server 2003 中，默认情况下，操作系统中不安装终端服务，需要通过添加/删除 Windows 组件来手动安装。终端服务最大的好处是允许多用户同时运行终端服务器的应用程序。

远程桌面主要是为了便于系统管理员远程管理服务器而推出的一项功能。该功能允许用户使用“远程桌面连接”程序连接到启用了远程桌面的计算机上。成功连接后，用户也可以运行远程计算机上的程序，管理远程计算机等，就好像是直接坐在远程计算机上操作一样。远程计算机接收用户在客户端计算机上鼠标、键盘的输入，而程序只在远程计算机上执行，远程计算机返回给客户端计算机的是其屏幕的显示结果。

远程桌面与终端服务的相同之处，它们都是 Windows 系统的组件，都可以运行远程计算机上的应用程序，实现对远程计算机的远程管理或控制，就像是操纵自己的本地计算机一样简单，速度也非常快。

远程桌面与终端服务的区别也是非常明显的。

(1) 远程桌面是完全免费的，而终端服务只有 120 天的使用期，超过这个免费使用期就需要购买许可证了。

(2) 远程桌面最多只允许两个管理员远程连接；而终端服务没有这个限制，只要购买了足够的许可证，有多少个用户同时登录一台服务器都是可以的。

第 13 章　利用 VMware Workstation 安装 Windows

学习目标

学习完本章后，能够了解虚拟机软件的作用，并掌握如何利用 VMware Workstation 从 ISO 镜像或安装 CD 安装 Windows Server 2003。

13.1　虚拟机概述

1. 什么是虚拟机

虚拟机（Virtual Machine）可以在一台物理计算机上模拟出若干台逻辑计算机，每台逻辑计算机可以单独运行而互不干扰，从而实现在一台物理计算机上同时运行多个操作系统，还可以利用多个操作系统构建网络。注意，本章所讲的虚拟机有别于 Java 虚拟机，Java 虚拟机表示不依赖操作系统平台运行的 Java 应用。

虚拟机体系结构如图 13-1 所示。安装虚拟机的物理计算机称为主机计算机（Host PC），物理计算机上运行的操作系统称为主机操作系统（Host OS），其中安装的虚拟机应用程序可以模拟出一个或多个虚拟机，在虚拟机上运行的操作系统称为客机操作系统（Client OS）。虚拟机软件可以在主机计算机上模拟出若干台虚拟机，虚拟机可以同时运行，可以像标准 Windows 应用程序那样相互切换。每个客机操作系统之间、客机操作系统和主机操作系统之间可以通过虚拟网卡连接成为一个局域网。

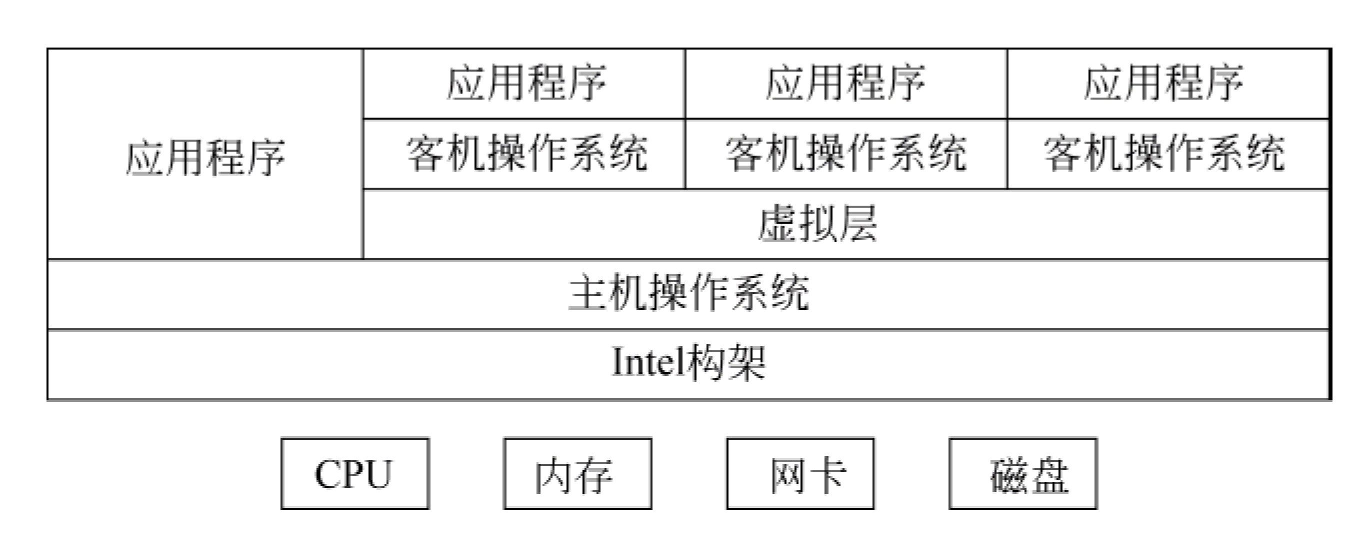


图 13-1　虚拟机体系结构

目前，基于 Intel 平台的虚拟机应用程序的典型产品有 VMware 的 Workstation、GSX Server、ESX Server 和 Microsoft 的 Virtual PC、Virtual Server 等。它们均可使用虚拟的 Intel x86 平台，同时运行多个操作系统和应用程序。虚拟机为客机操作系统提供了一整套虚拟的 Intel x86 兼容硬件，其虚拟了物理计算机所拥有的全部设备，包括主板芯片、CPU、内存、SCSI 和 IDE 磁盘设备、各种接口和显示设备等。每个虚拟机都可以被独立地封装到一个文件中，可以实现虚拟机的灵活迁移。

使用虚拟技术有两个好处：一方面是使用虚拟机技术把一个物理计算机虚拟成若干个独立的逻辑计算机；另一方面是使用网格技术把若干个分散的物理计算机虚拟为一个大的逻辑计算机。虚拟机主要采用分区技术，分区能够将物理系统资源划分成多个不同、单独的部分，各部分彼此独立操作，每个分区只能占用一定的系统资源。

2. VMware 虚拟机简介

VMware 公司提供工作站、部门服务器和企业机服务器的虚拟机解决方案，分别是 VMware Workstation、VMware GSX Server 和 VMware ESX Server。

VMware ESX Server 属于高阶产品，它本身就是一个操作系统，并不需要 Host OS 的支持。它能够在高性能的环境中提供服务器整合和分区管理，为用户提供先进的资源管理功能，以及带有远程 Web 管理和客户端管理功能。

VMware GSX Server 需要安装在 Host OS 上，支持 Windows 2000 Server 以上的 Windows 系统或者 Linux(如 RedHat、SUSE、Mandrake 等)，具有远程 Web 管理和客户端管理功能。

VMware Workstation 提供本地的虚拟服务器，功能与 VMware GSX Server 没有太大的区别，但没有 Web 远程管理和客户端管理功能。

13.2 创建并配置一台虚拟机

获取 VMware Workstation 8.0 安装包，并安装。

打开 VMware Workstation 8.0，主界面如图 13-2 所示。

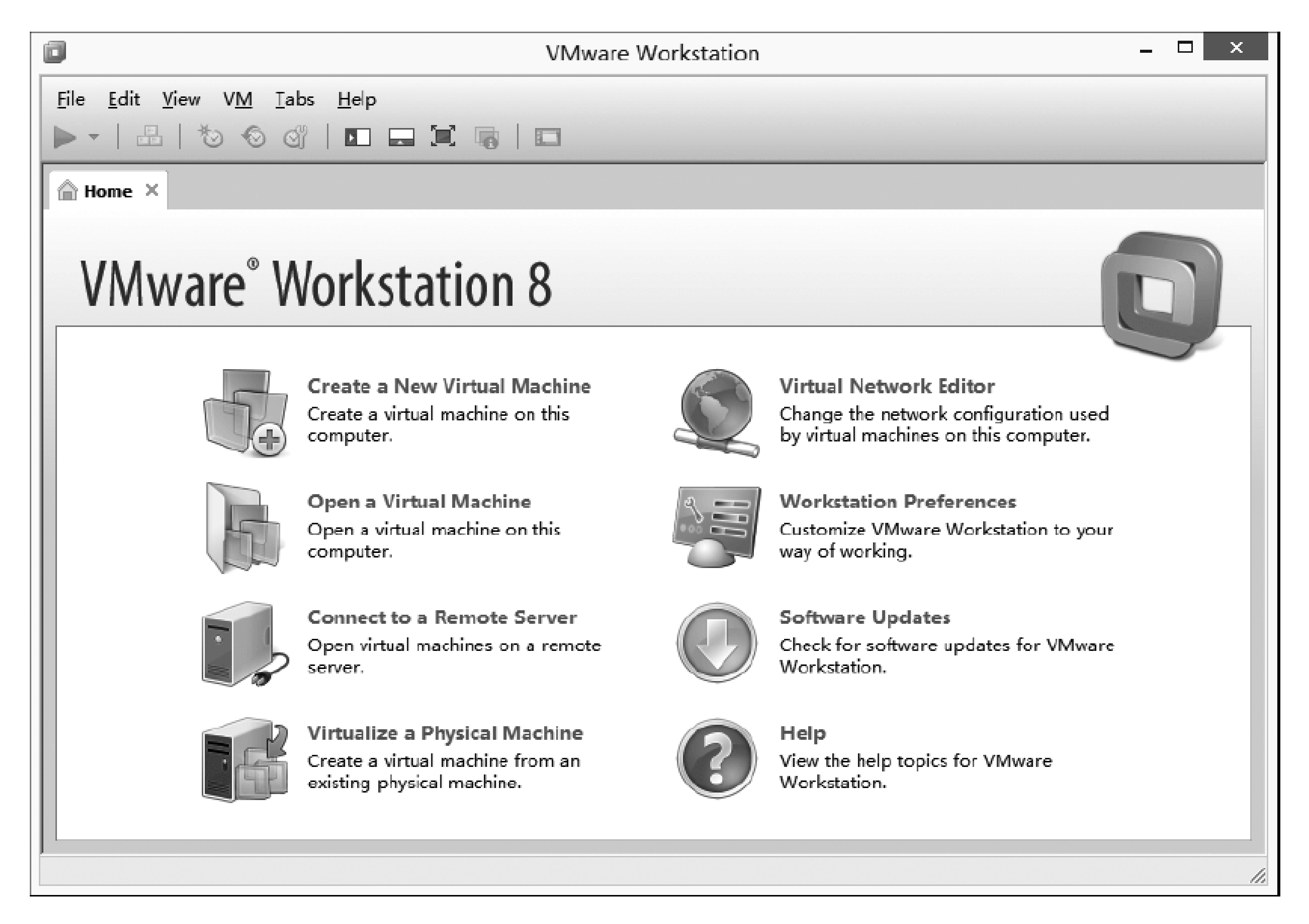


图 13-2 VMWare Workstation 8.0 主界面

单击 Create a New Virtual Machine，创建一个新的虚拟机，新建虚拟机向导如图 13-3 所示。



图 13-3 新建虚拟机向导

选择 Custom(advanced)单选按钮，单击 Next 按钮，选择虚拟机硬件兼容性，如图 13-4 所示。



图 13-4 选择虚拟机硬件兼容性

选择 Workstation 8.0，单击 Next 按钮，选择安装操作系统的安装源，如图 13-5 所示。

选择的操作系统为 Microsoft Windows，版本为 Windows Server 2003 Enterprise Edition，如图 13-6 所示。

指定虚拟机名称和存放的位置，最好是指定到可用空间大的分区，例如 G:\class vm 2003 server\，如图 13-7 所示。

指定虚拟机的处理器配置，即处理器个数及每个处理器为几核，如图 13-8 所示。

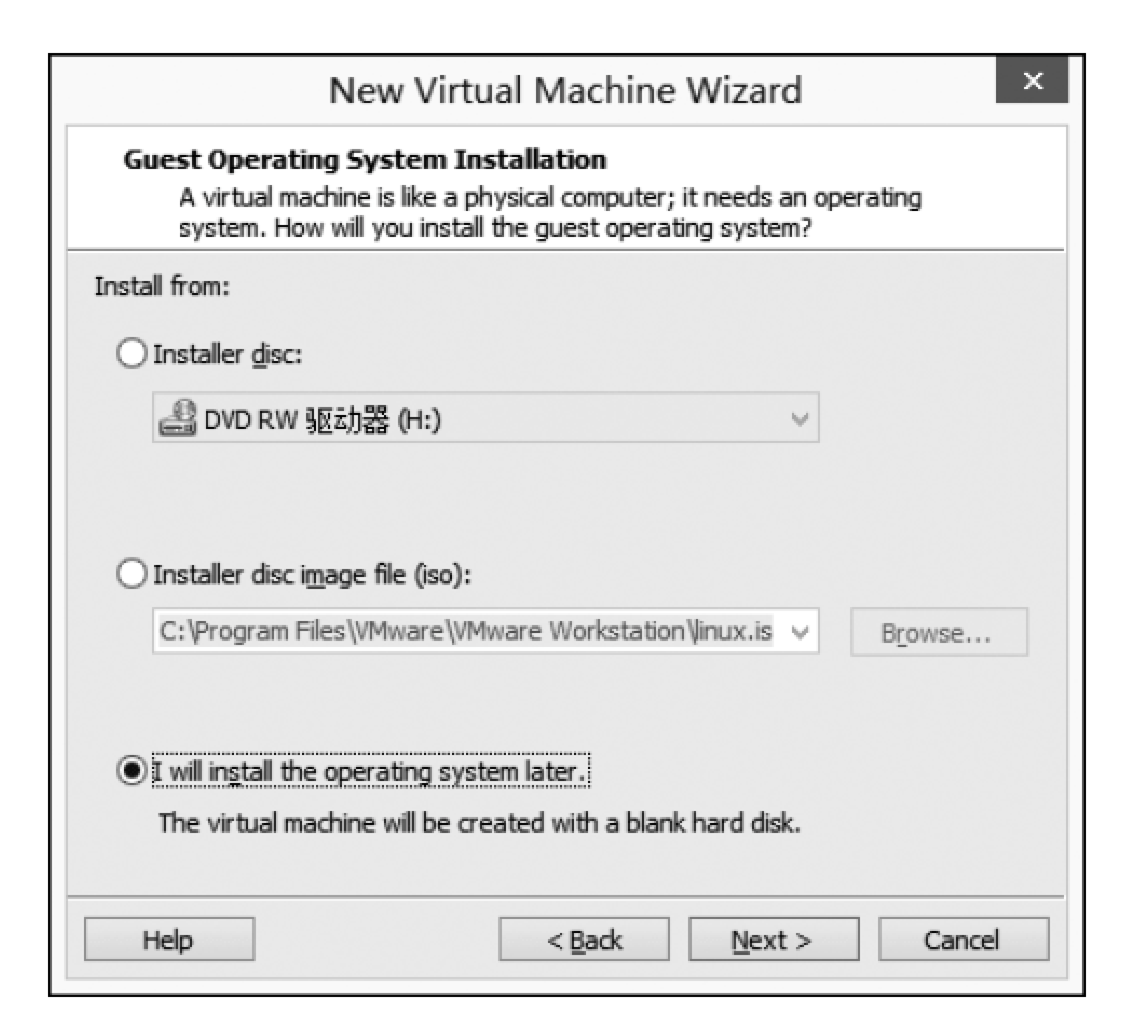


图 13-5 选择操作系统的安装源

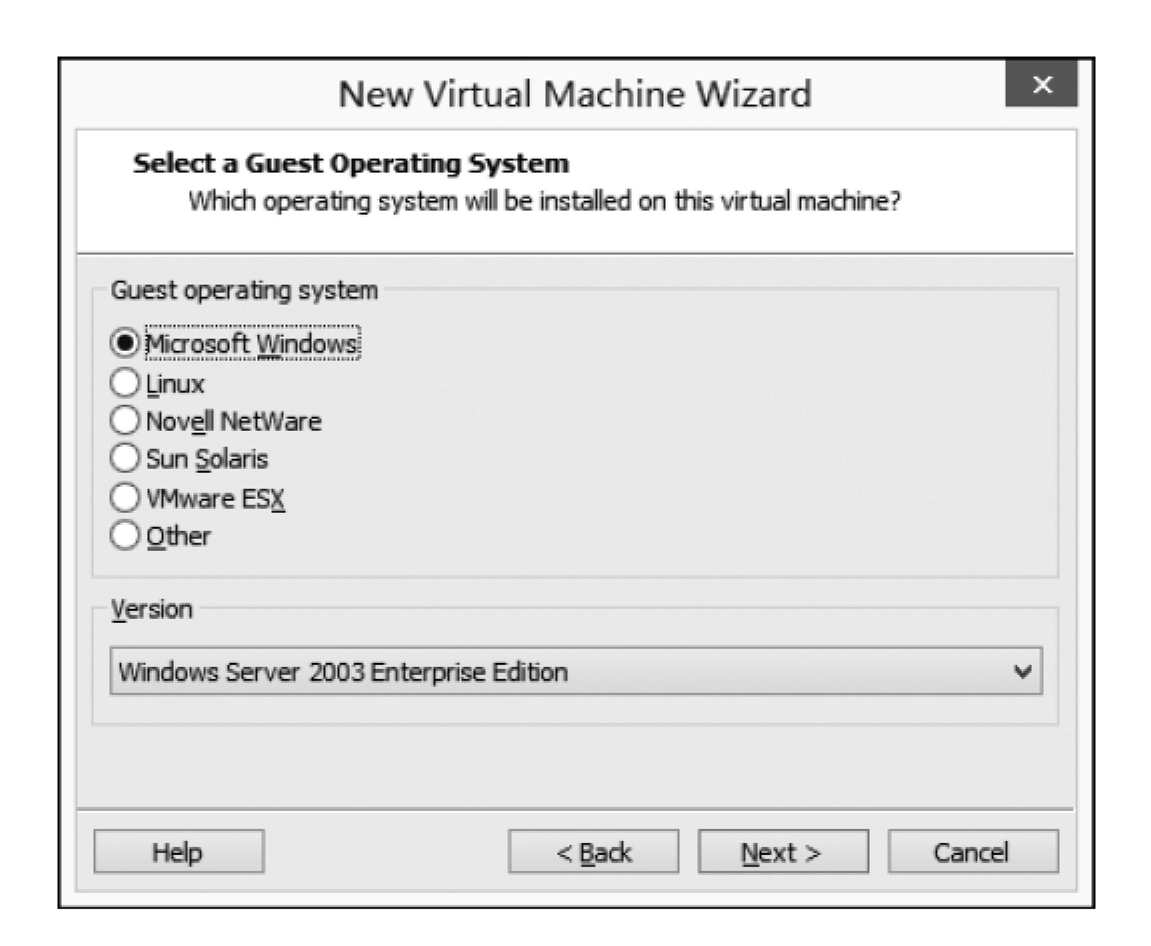


图 13-6 操作系统及其版本选择

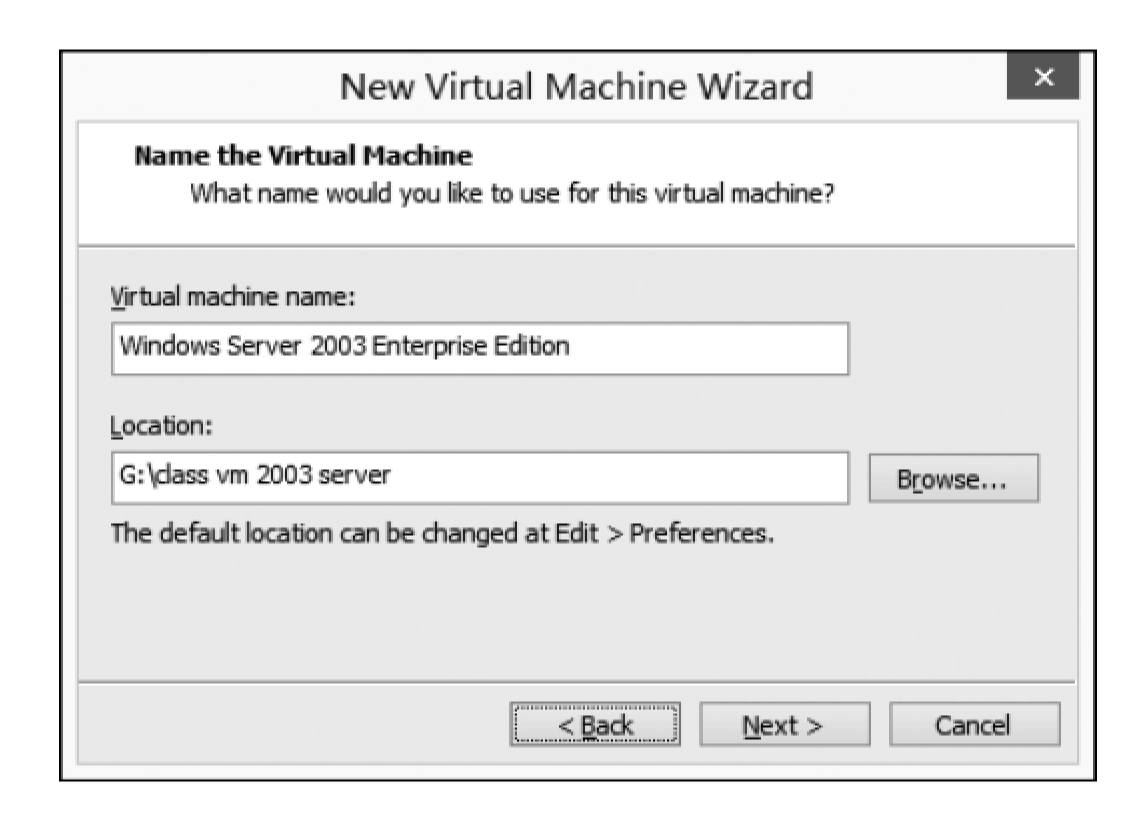


图 13-7 指定虚拟机的名称和存放位置

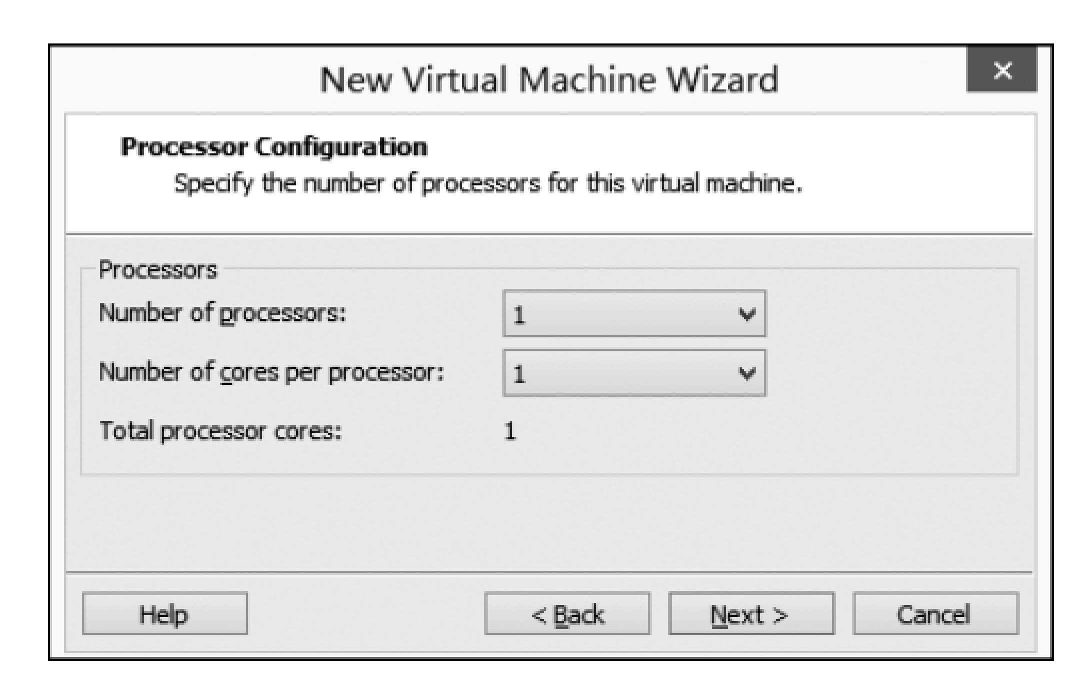


图 13-8　指定处理器的配置

指定虚拟机的内存大小，建议使用推荐的内存大小，如图 13-9 所示。



图 13-9　指定虚拟机的内存大小

指定虚拟机的网络连接方式，在此使用 NAT，如图 13-10 所示。

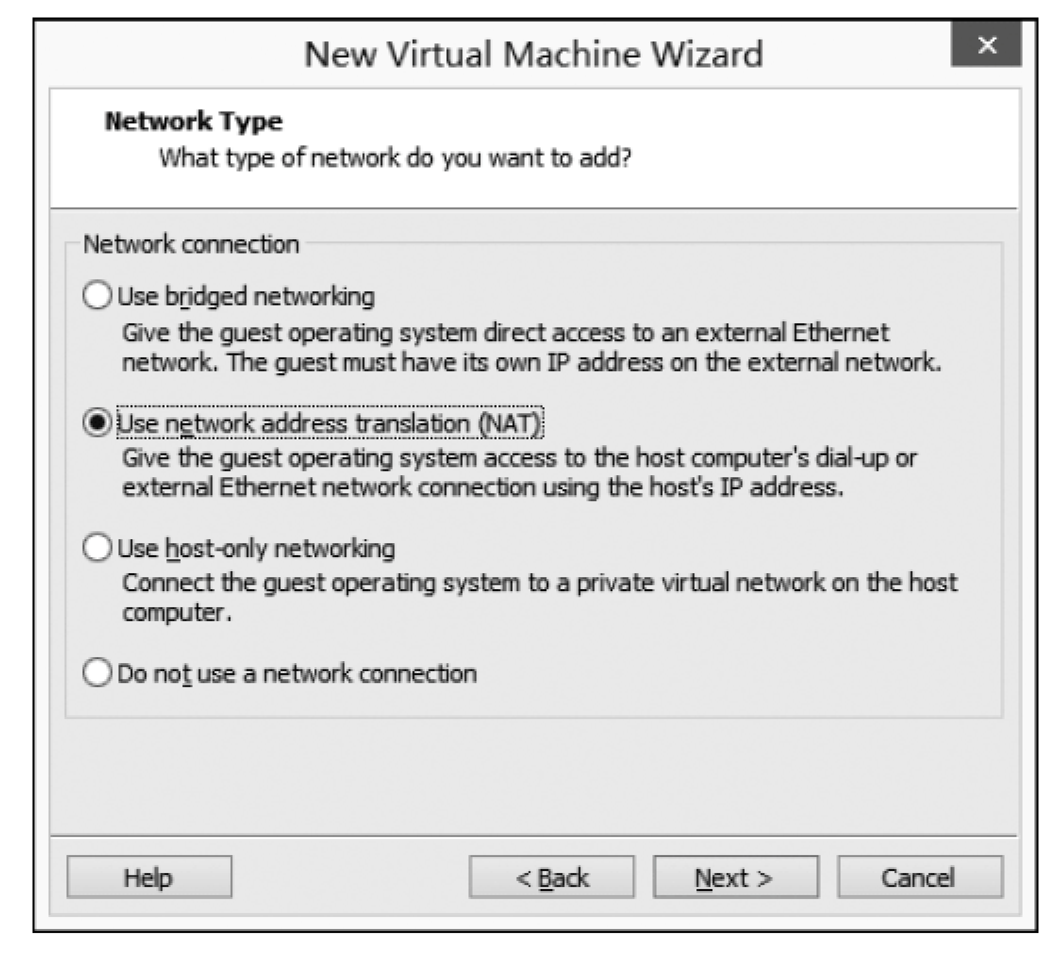


图 13-10　指定虚拟机网络连接方式

选择 I/O 控制器的类型，默认选项即可，如图 13-11 所示。

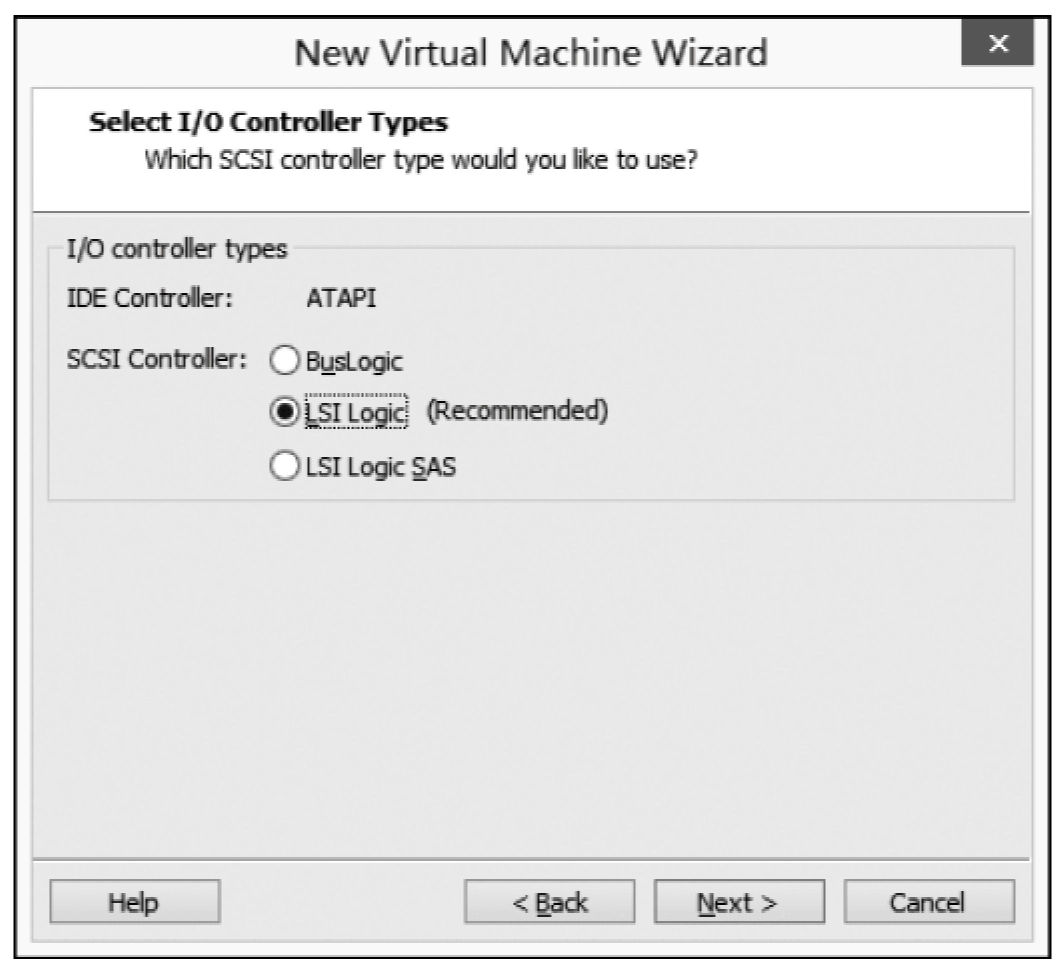


图 13-11 指定 I/O 控制器的类型

选择硬盘，选择 Create a new virtual disk（创建新的虚拟硬盘）单选按钮，如图 13-12 所示。



图 13-12 创建新的虚拟硬盘

选择硬盘的类型，默认选项即可，如图 13-13 所示。

指定虚拟机的虚拟硬盘容量大小，例如 40GB，如图 13-14 所示。

指定虚拟硬盘的存储位置和文件名，最好指定到虚拟机的存放位置，例如 G:\class vm 2003 server\，如图 13-15 所示。

单击 Next 按钮，出现虚拟机的配置摘要，如图 13-16 所示。

单击 Finish 按钮，完成虚拟机创建向导，虚拟机创建完成的界面如图 13-17 所示。

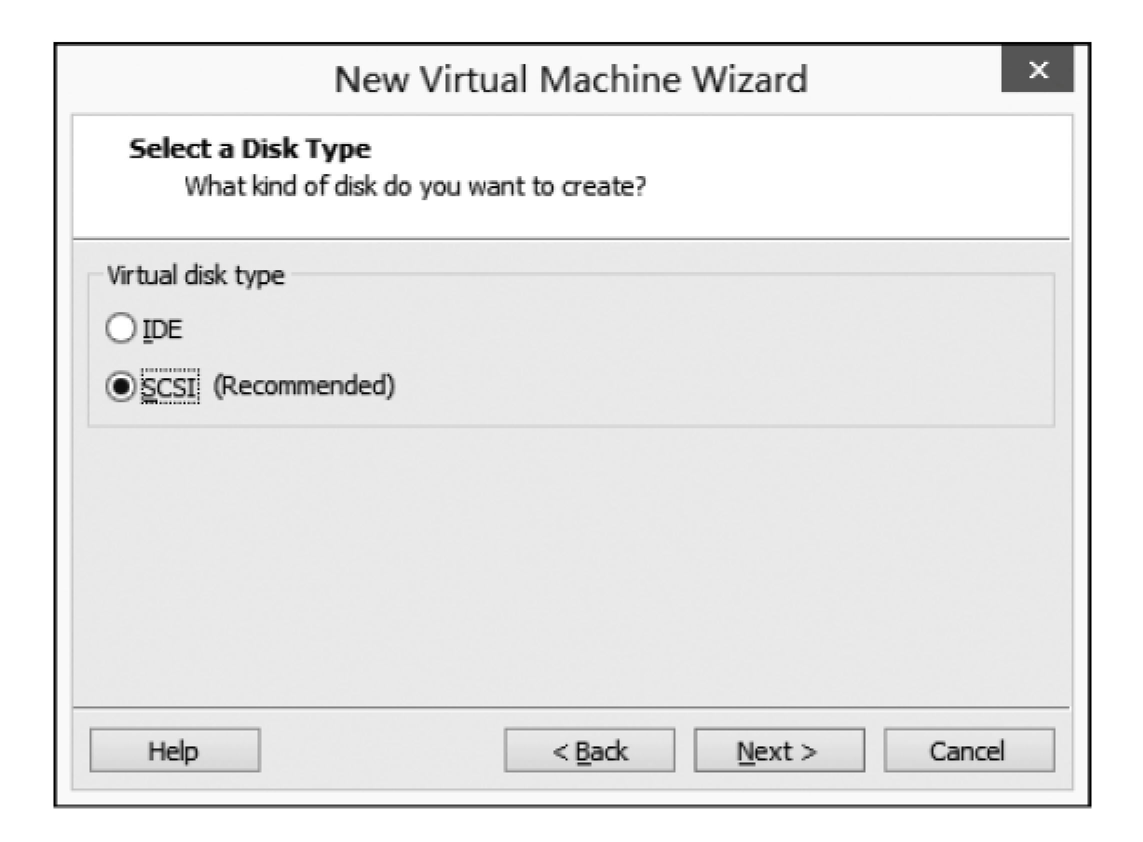


图 13-13　选择虚拟硬盘的类型



图 13-14　指定虚拟硬盘容量大小



图 13-15　指定虚拟硬盘的文件名和存储位置

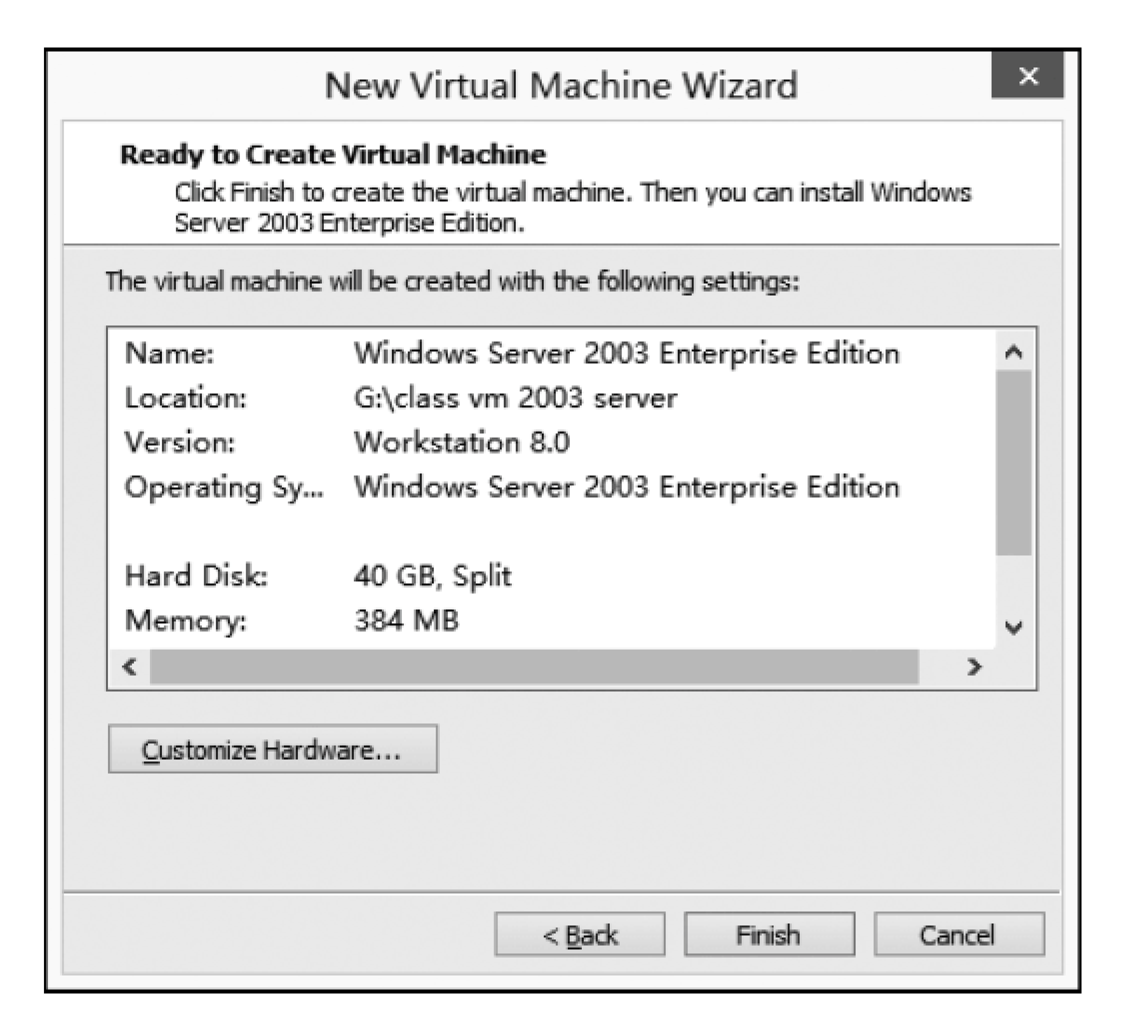


图 13-16 虚拟机的配置摘要

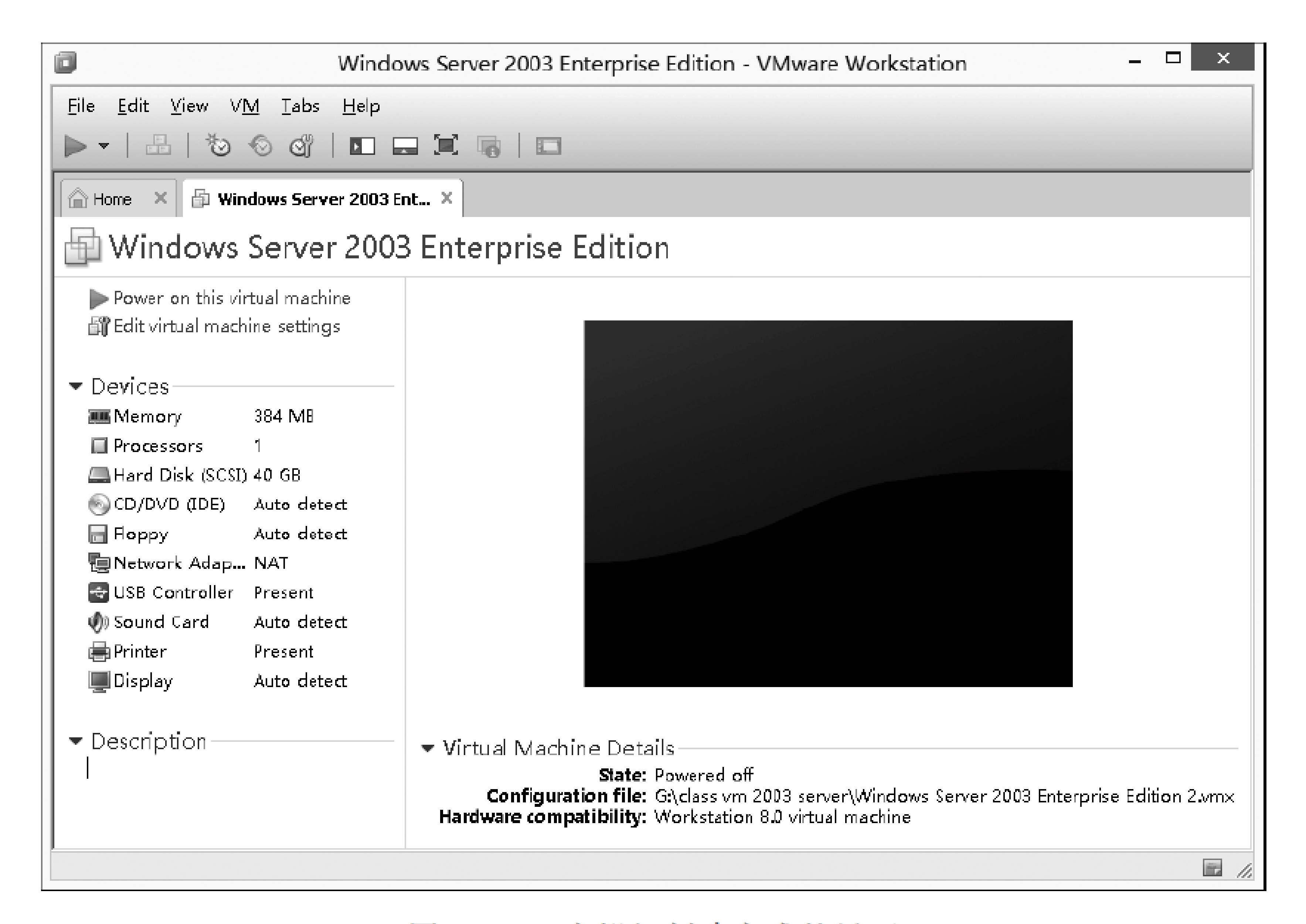


图 13-17 虚拟机创建完成的界面

13.3 开始安装操作系统

如果使用 Windows 的 ISO 镜像文件安装操作系统，单击图 13-16 中的 CD/DVD(IDE)，指定 ISO 镜像文件的位置(请提前将 Windows 的 ISO 镜像文件下载到本地磁盘上)，如图 13-18 所示。

单击 OK 按钮，返回图 13-17 的主界面，单击 Power on this vitual machine，即可在虚

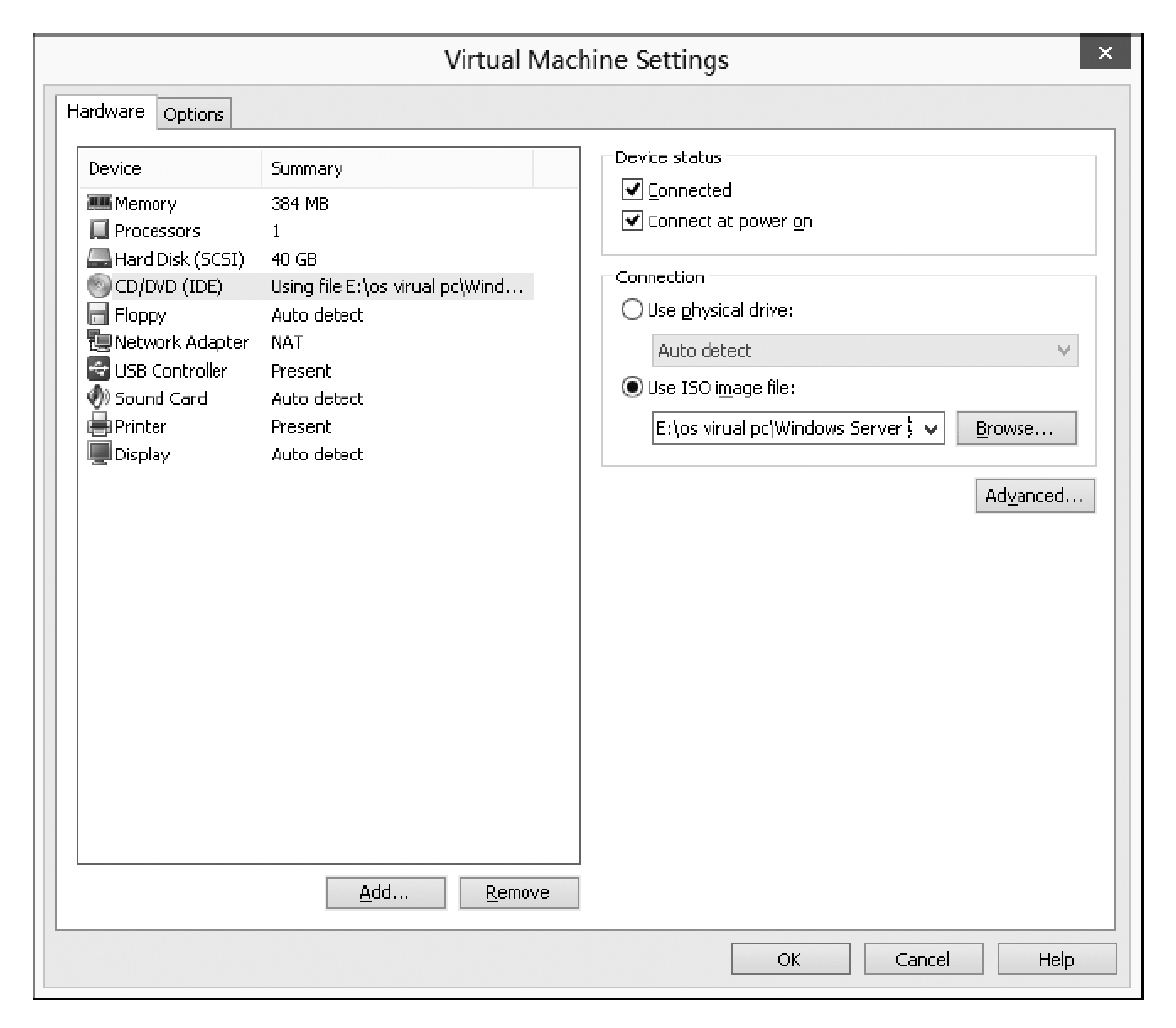


图 13-18　指定 ISO 镜像文件的位置

拟机上从光盘(ISO 镜像文件)开始安装操作系统,Windows Server 2003 欢迎安装界面如图 13-19 所示。

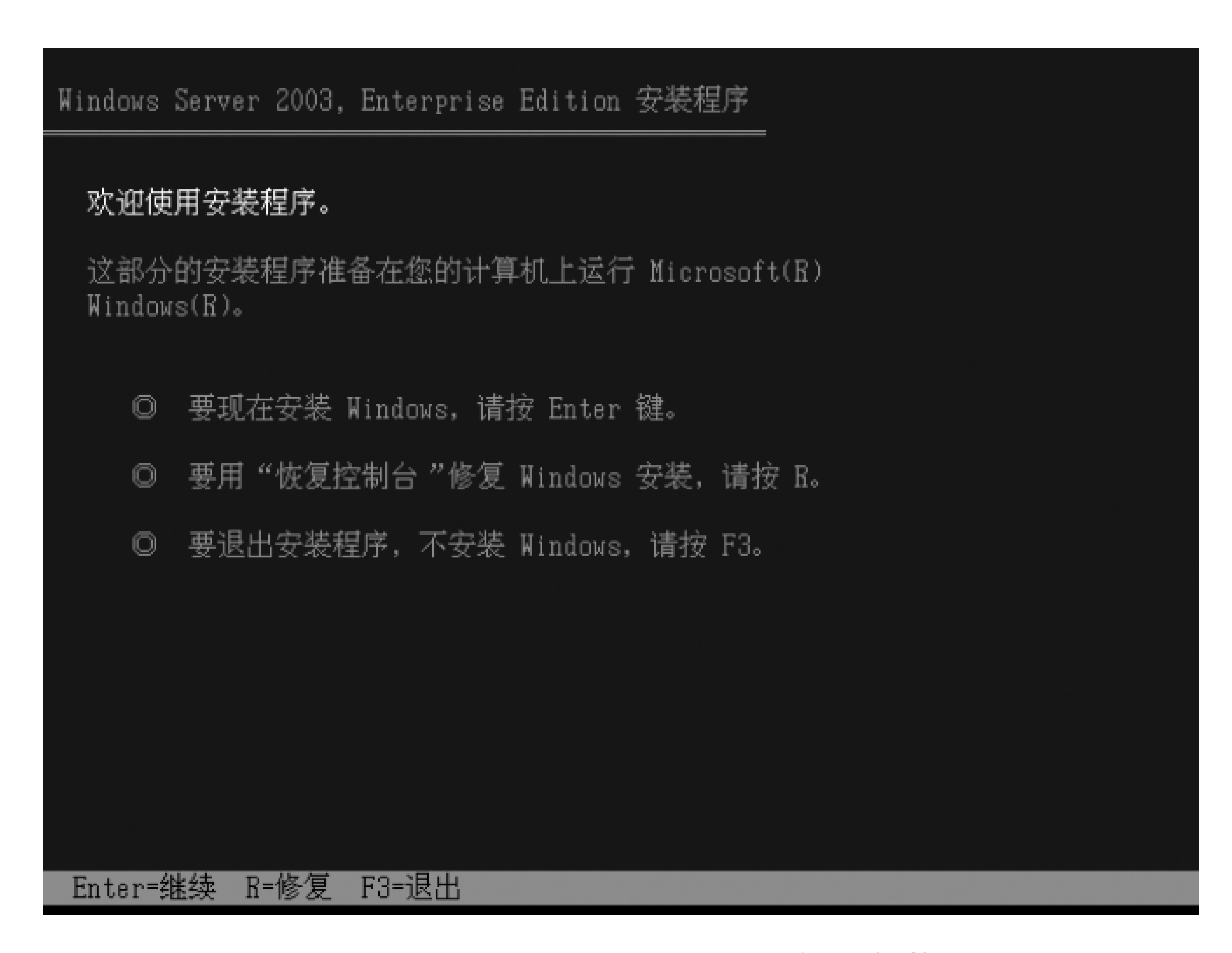


图 13-19　Windows Server 2003 欢迎安装界面

要现在开始安装 Windows,请按 Enter 键,出现 Windows 授权协议界面,如图 13-20 所示。

按 F8 功能键,同意许可协议,之后出现如图 13-21 所示的磁盘分区界面。

接下来创建磁盘分区。虽然可以直接按 Enter 键在未划分的空间上安装 Windows,

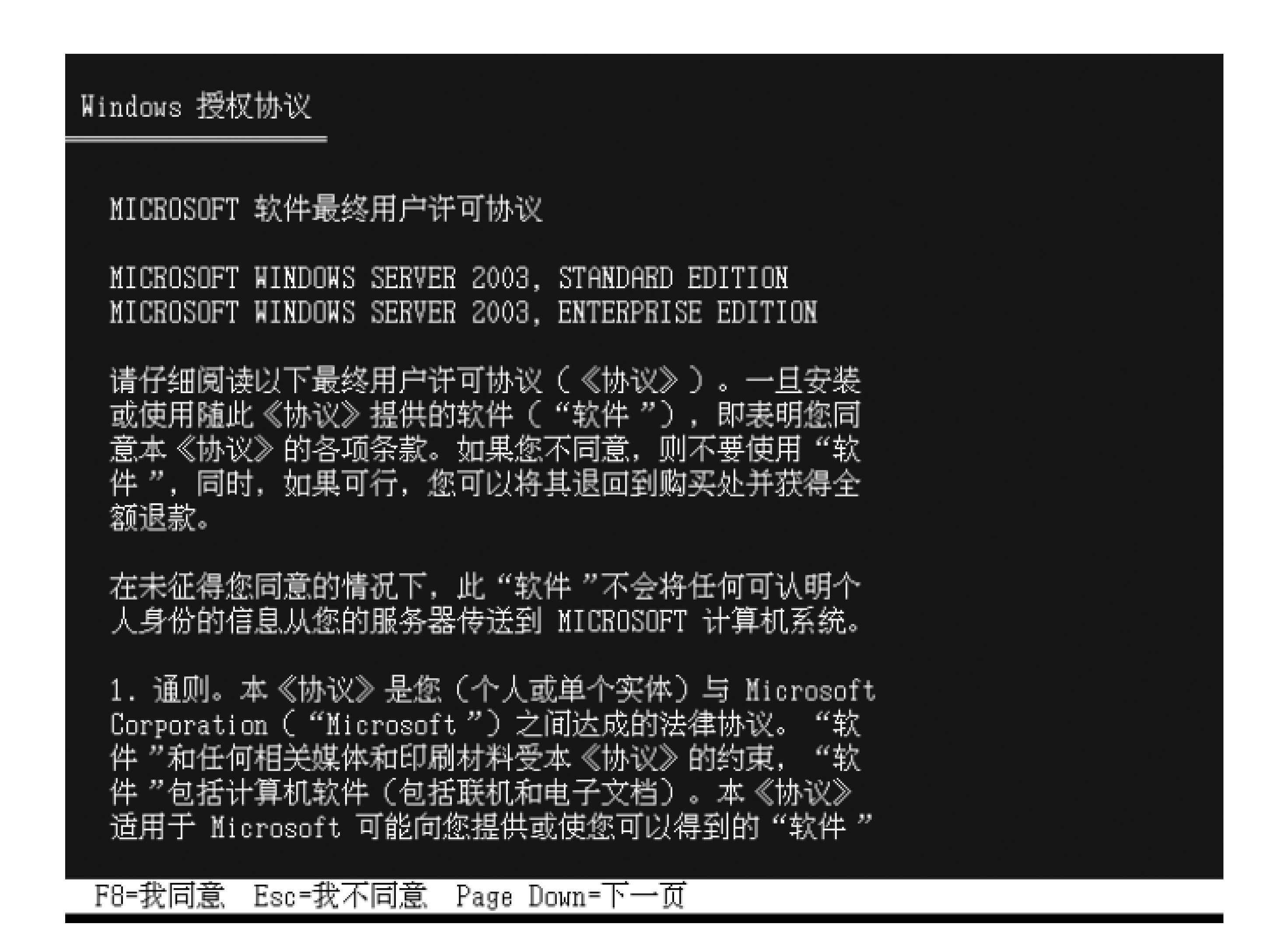


图 13-20　Windows 授权协议界面

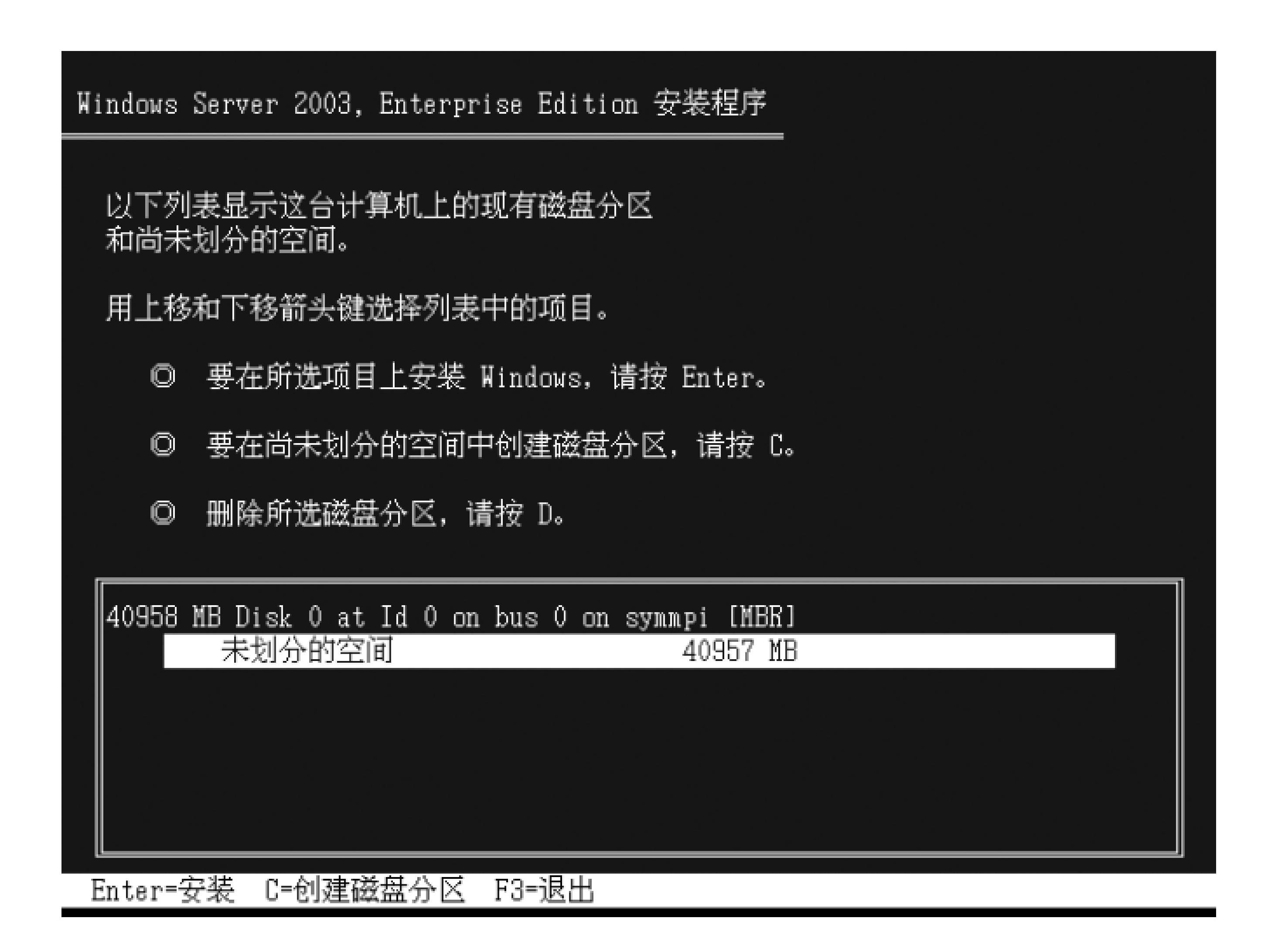


图 13-21　磁盘分区界面

但不建议这样做，这样做的后果是系统安装完成后，整个系统默认将只有一个 C 盘。

要在尚未划分的空间中创建磁盘分区，请按 C 键，在如图 13-22 所示的界面中，指定要创建的磁盘分区大小，例如 20 000MB。

按 Enter 键完成分区 1 的创建，如图 13-23 所示。

可以在未划分的空间中创建新的分区，也可按 D 键删除已创建的分区。

在刚才创建的分区 1 上安装 Windows，按 Enter 键。

格式化磁盘分区，选择“用 NTFS 文件系统格式化磁盘分区(快)”，如图 13-24 所示。

安装程序正在格式化磁盘分区，如图 13-25 所示。

Windows Server 2003, Enterprise Edition 安装程序

您已要求安装程序在 40958 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR]
上创建新的磁盘分区。

◎ 要创建新磁盘分区，请在下面输入大小，然后按 Enter。

◎ 要回到前一个屏幕而不创建新磁盘分区，请按 Esc。

最小新磁盘分区为 7 MB。
最大新磁盘分区为 40950 MB。
创建磁盘分区大小(单位 MB)： 20000_

Enter=创建 Esc=取消

图 13-22 指定要创建的磁盘分区大小

Windows Server 2003, Enterprise Edition 安装程序

以下列表显示这台计算机上的现有磁盘分区
和尚未划分的空间。

用上移和下移箭头键选择列表中的项目。

◎ 要在所选项目上安装 Windows，请按 Enter。

◎ 要在尚未划分的空间中创建磁盘分区，请按 C。

◎ 删除所选磁盘分区，请按 D。

40958 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR]
C: 分区 1 [新的(未使用)] 19998 MB (19997 MB 可用)
未划分的空间 20960 MB

Enter=安装 D=删除磁盘分区 F3=退出

图 13-23 完成分区 1 的创建

Windows Server 2003, Enterprise Edition 安装程序

选择的磁盘分区没有经过格式化。安装程序
将立即格式化这个磁盘分区。

使用上移和下移箭头键选择所需的文件系统，然后请按 Enter。

如果要为 Windows 选择不同的磁盘分区，请按 Esc。

用 NTFS 文件系统格式化磁盘分区（快）
用 FAT 文件系统格式化磁盘分区（快）
用 NTFS 文件系统格式化磁盘分区
用 FAT 文件系统格式化磁盘分区

Enter=继续 Esc=取消

图 13-24 格式化磁盘分区

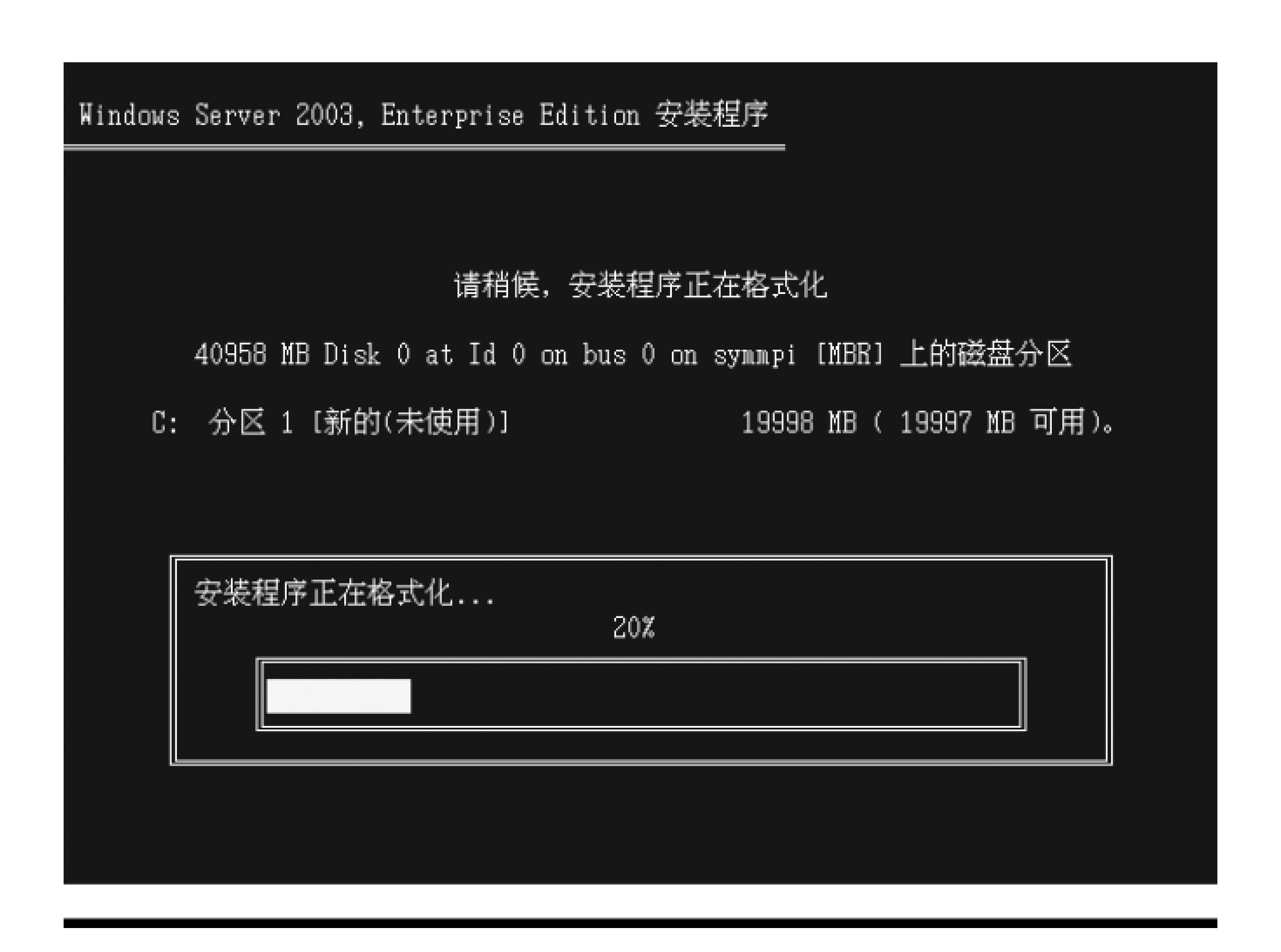


图 13-25 安装程序正在格式化磁盘分区

格式化完成后，开始复制文件并重新启动。

开始进入图形界面安装阶段，如图 13-26 所示。



图 13-26 图形界面安装向导

指定区域和语言选项，输入姓名和单位，如图 13-27 所示。

输入产品密钥，如图 13-28 所示。

选择授权模式，一般选择每服务器模式，如图 13-29 所示。

每服务器模式限制同时访问本机的客户机数量，每服务器模式适合在只有一台或少量服务器的网络中使用。



图 13-27　输入姓名、单位信息

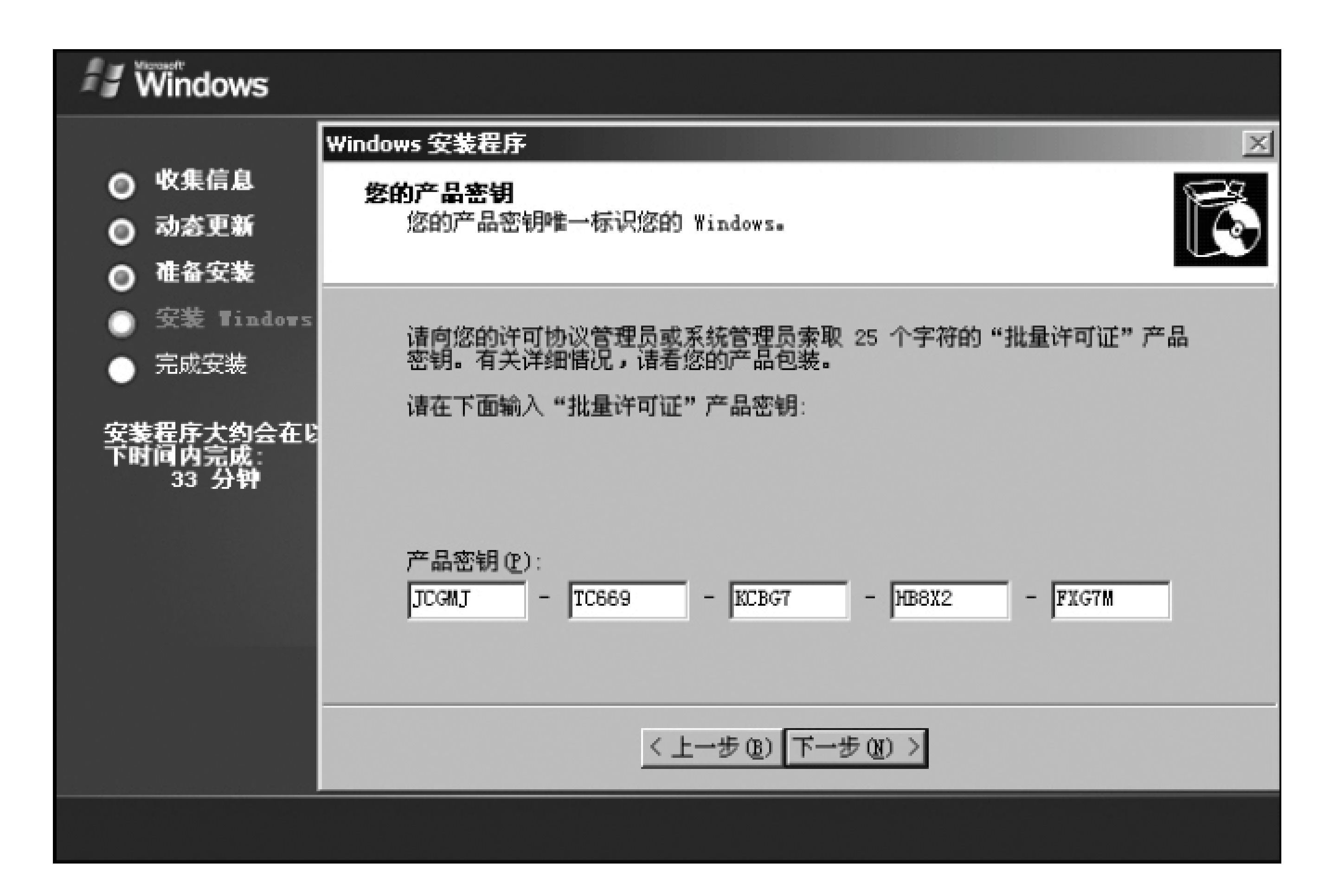


图 13-28　输入产品密钥

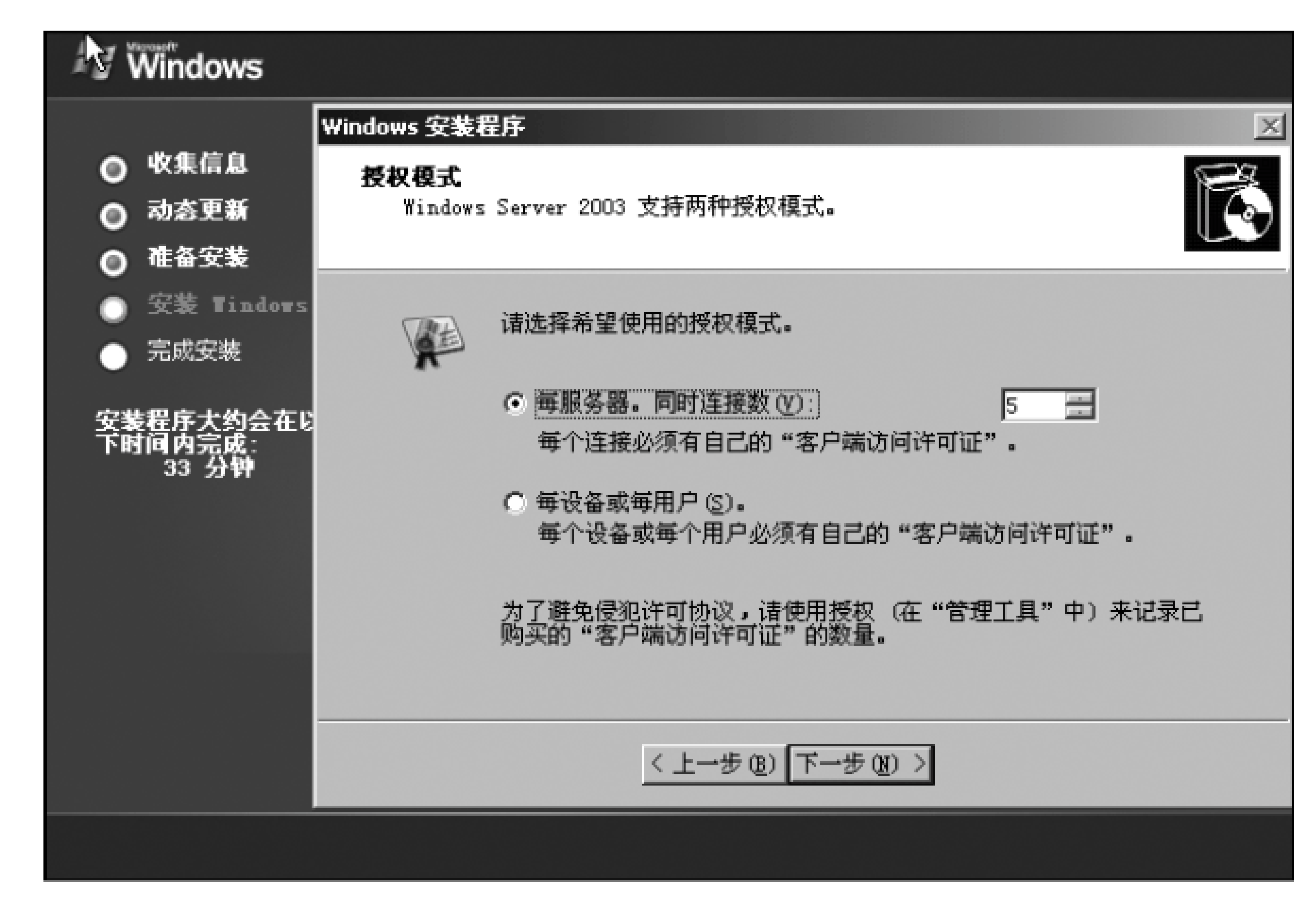


图 13-29　选择授权模式

每设备模式不限制，但要求每台客户机都要购买“客户端访问许可证”，每设备模式适合于有多台服务器的网络中使用。

输入计算机名称和管理员密码，如图 13-30 所示。



图 13-30　输入计算机名称和管理员密码

计算机名称最好自己定义一个，方便记忆和查找。

接下来设置日期和时间，设置网络属性，选择“典型设置”或者“自定义设置”，在此选择“自定义设置”，如图 13-31 所示。



图 13-31　选择“自定义设置”选项

配置网络组件，选择“Internet 协议(TCP/IP)”，如图 13-32 所示。

单击“属性”按钮，根据网络实际情况，选择“自动获得 IP 地址”(DHCP)或者“使用下

面的 IP 地址”(手工静态分配 IP 地址),如图 13-33 所示。

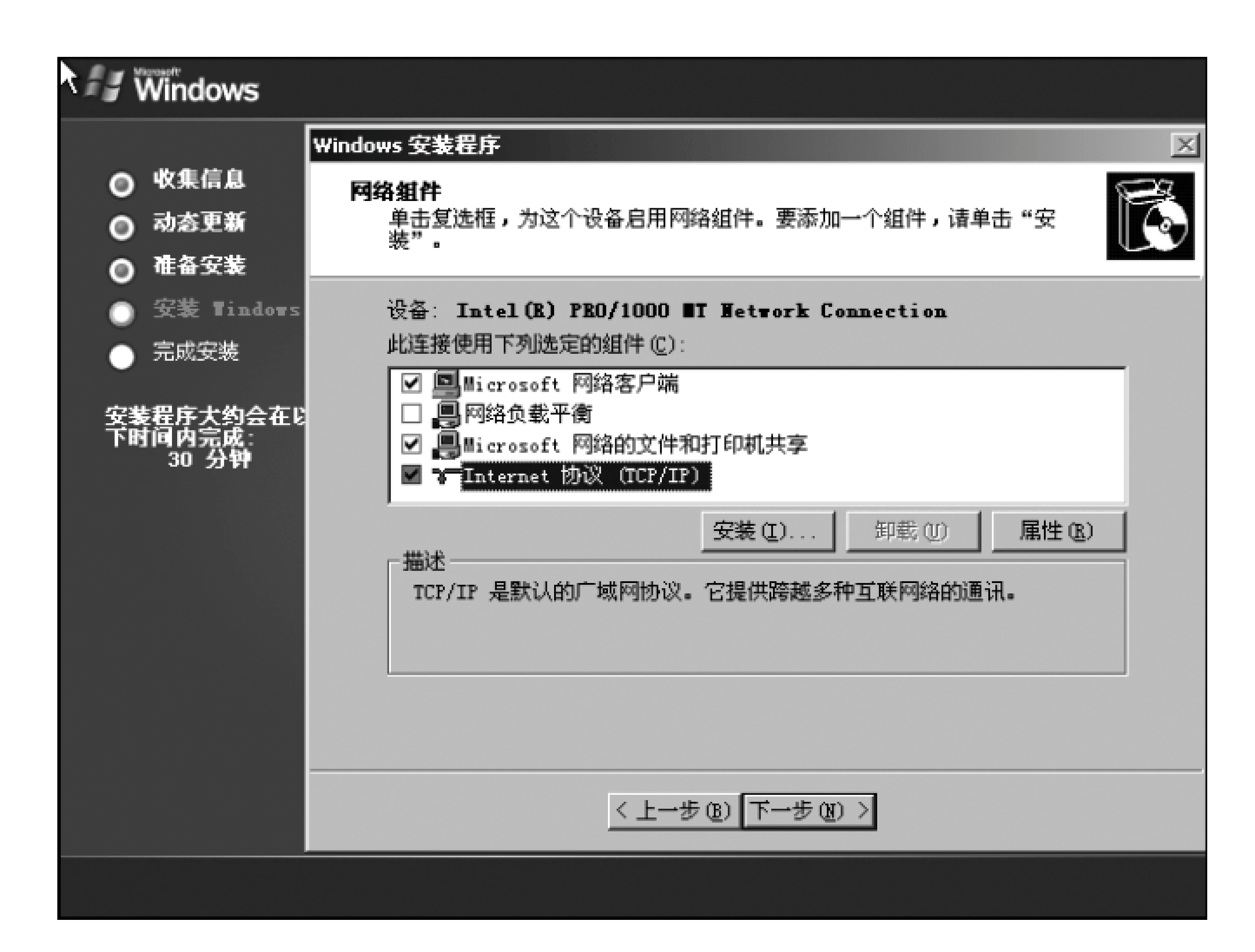


图 13-32　网络组件

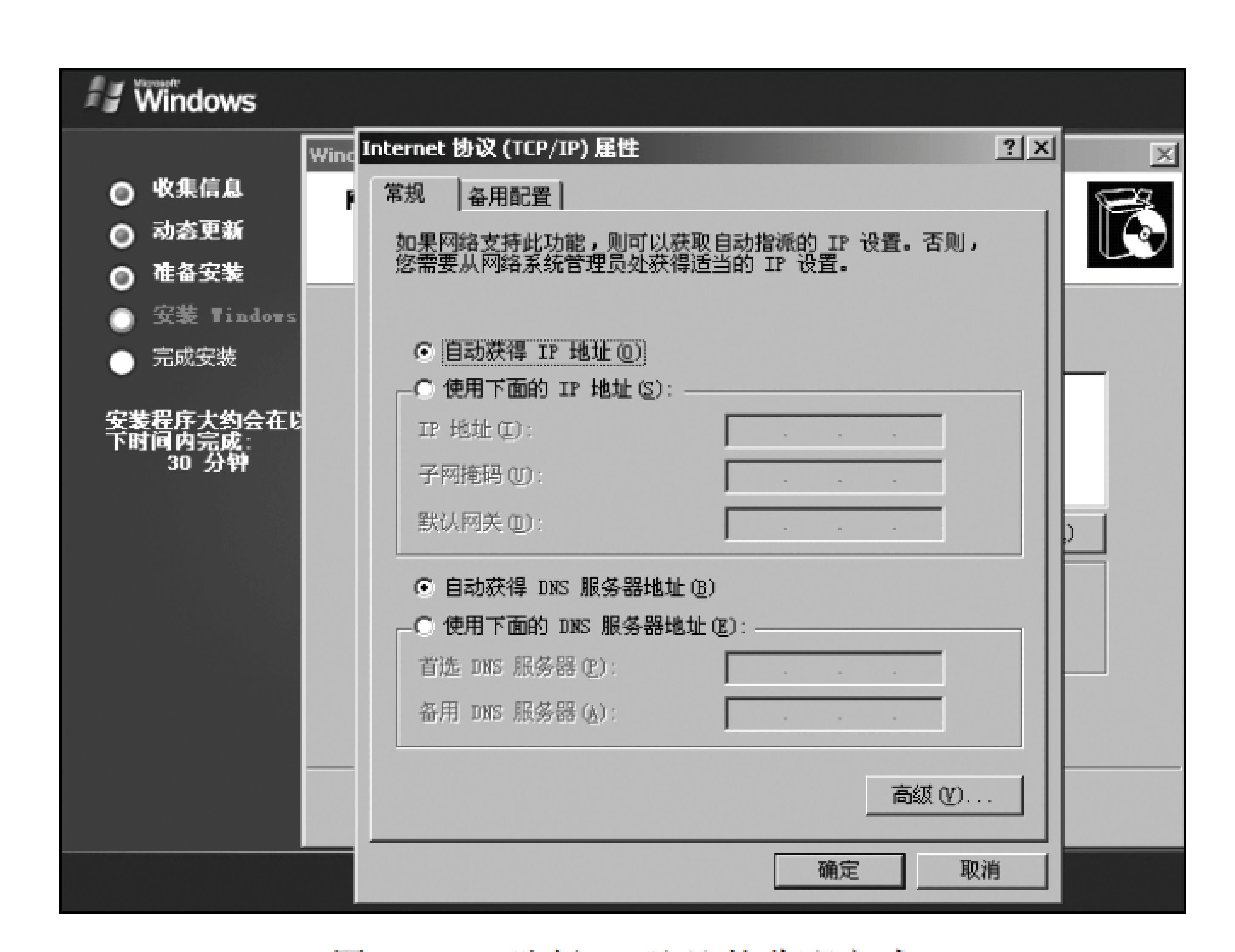


图 13-33　选择 IP 地址的分配方式

选择工作组或计算机域,保持默认的工作组 WORKGROUP,如图 13-34 所示。

完成后续的安装过程,重启后,系统安装完成。

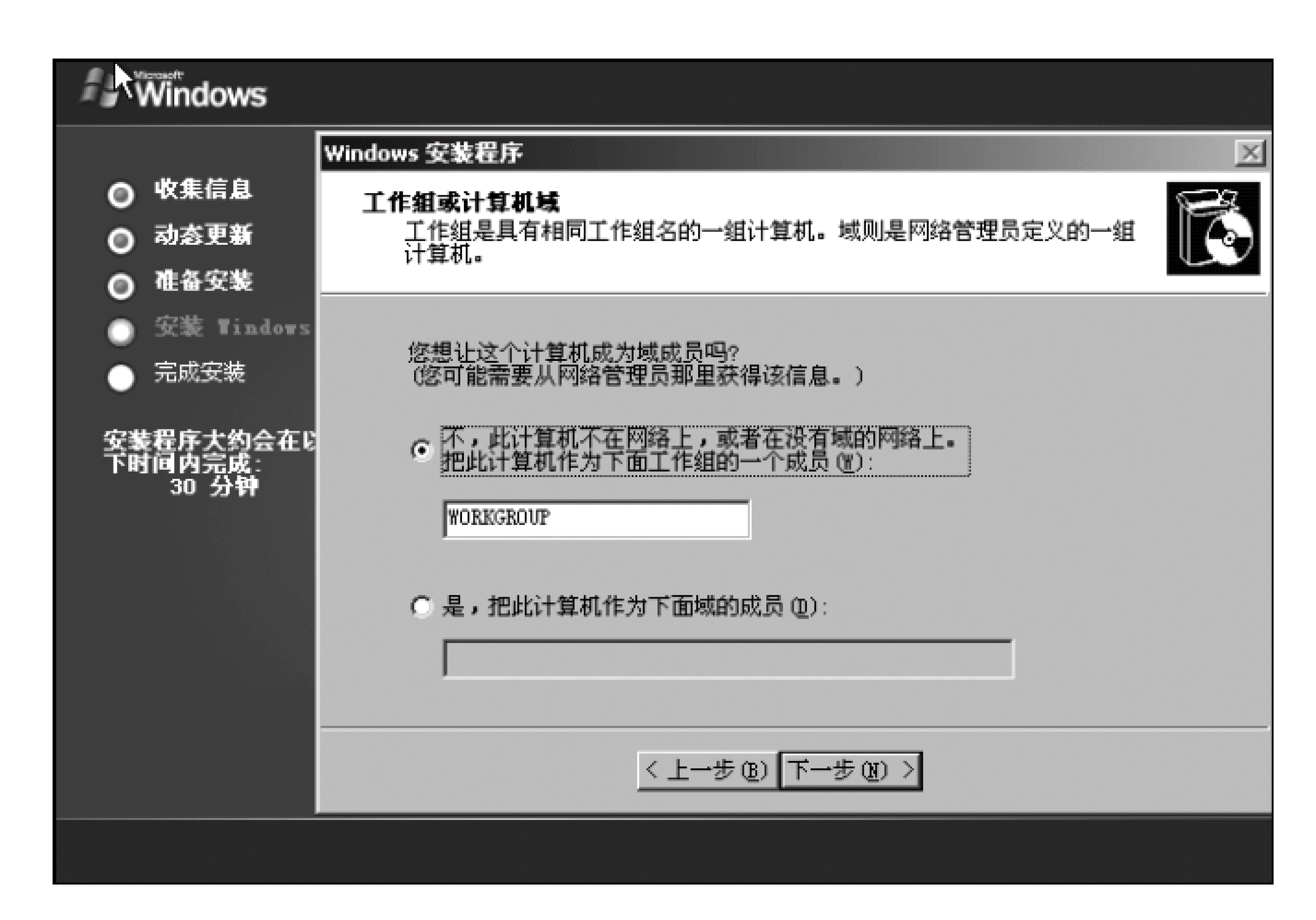


图 13-34　选择工作组或计算机域

13.4　虚拟机快捷键

虚拟机快捷键如表 13-1 所示。

表 13-1　虚拟机快捷键

快 捷 键	功　　能
Ctrl+B	开机
Ctrl+E	关机
Ctrl+R	重启
Ctrl+Z	挂起
Ctrl+N	新建一个虚拟机
Ctrl+O	打开一个虚拟机
Ctrl+F4	关闭所选择虚拟机的概要或者控制视图。如果虚拟机开着，一个确认对话框将出现
Ctrl+D	编辑虚拟机配置
Ctrl+G	为虚拟机捕获鼠标和键盘焦点
Ctrl+P	编辑参数
Ctrl+Alt+Enter	进入全屏模式
Ctrl+Alt	返回正常(窗口)模式
Ctrl+Alt+Tab	当鼠标和键盘焦点在虚拟机中时，在打开的虚拟机中切换
Ctrl+Tab	当鼠标和键盘焦点不在虚拟机中时，在打开的虚拟机中切换。VMware Workstation 应用程序必须在活动应用状态上
Ctrl+Shift+Tab	当鼠标和键盘焦点不在虚拟机中时，在打开的虚拟机中切换。VMware Workstation 应用程序必须在活动应用状态上

13.5 VMware WorkStation 的网络连接方式

在学习 VMware 的网络模型之前，先介绍 VMware 的几个虚拟设备。

VMnet0：VMware 用于虚拟桥接网络下的虚拟交换机。

VMnet1：VMware 用于虚拟 Host-Only 网络下的虚拟交换机。

VMnet8：VMware 用于虚拟 NAT 网络下的虚拟交换机。

VMware Network Adapter VMnet1：Host 用于与 Host-Only 虚拟网络进行通信的虚拟网卡。

VMware Network Adapter VMnet8：Host 用于与 NAT 虚拟网络进行通信的虚拟网卡。

VMware 网络连接的方式主要有桥接、NAT、主机网络(Host-Only)。

1. 使用桥接网络

使用 VMnet0 虚拟交换机，此时虚拟机相当于网络上的一台独立计算机，与主机一样，拥有一个独立的 IP 地址，其网络拓扑如图 13-35 所示，使用桥接方式，A、A1、A2、B 可互访。

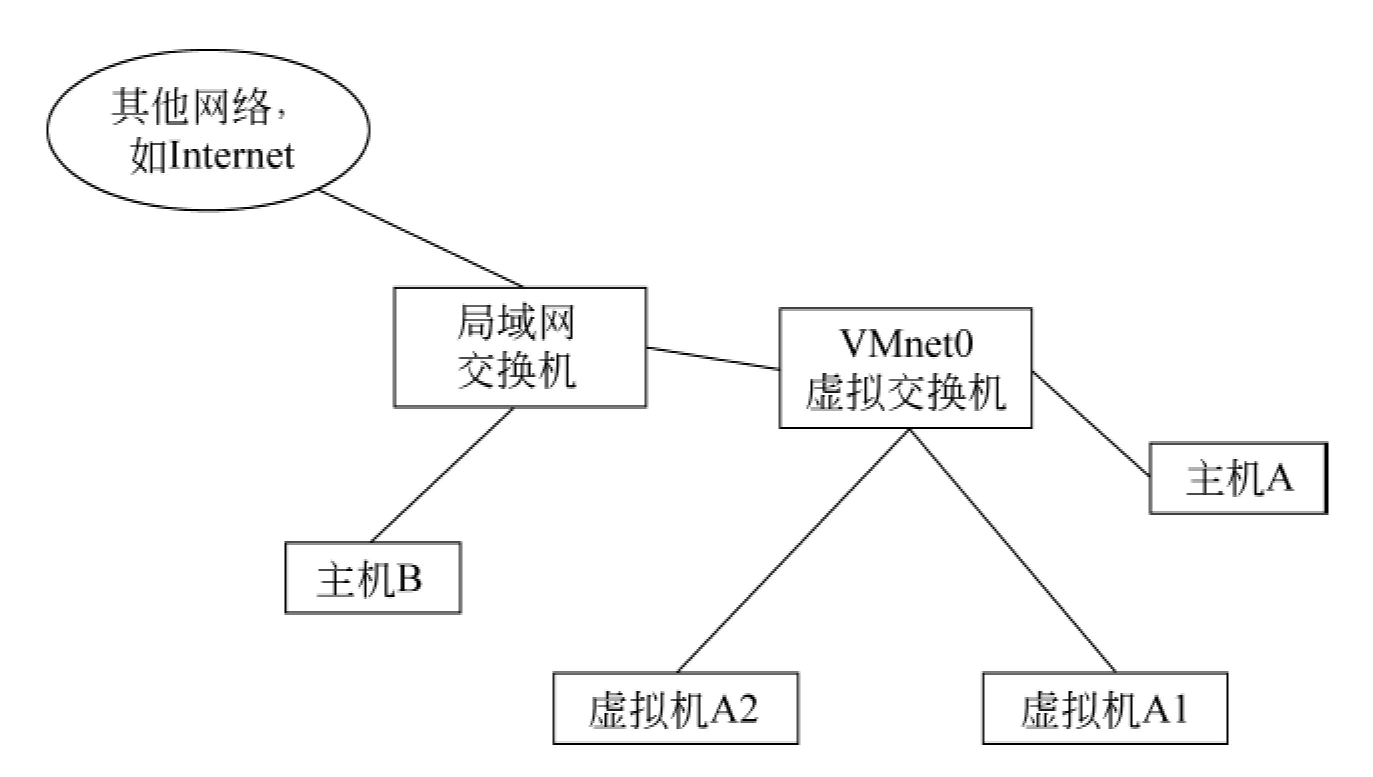


图 13-35 桥接方式网络拓扑示意图

2. NAT

使用 VMnet8 虚拟交换机，此时虚拟机可以通过主机单向访问网络上的其他工作站，其他工作站不能访问虚拟机。其网络拓扑如图 13-36 所示，使用 NAT 方式，A1、A2 可以访问 B，但 B 不可以访问 A1、A2。但 A、A1、A2 可以互访。

3. 使用主机网络

使用 VMnet1 虚拟交换机，此时虚拟机只能与虚拟机、主机互访，也就是虚拟机不能访问 Internet，其网络拓扑如图 13-37 所示，使用 Host 方式，A、A1、A2 可以互访，但 A1、A2 不能访问 B，也不能被 B 访问。

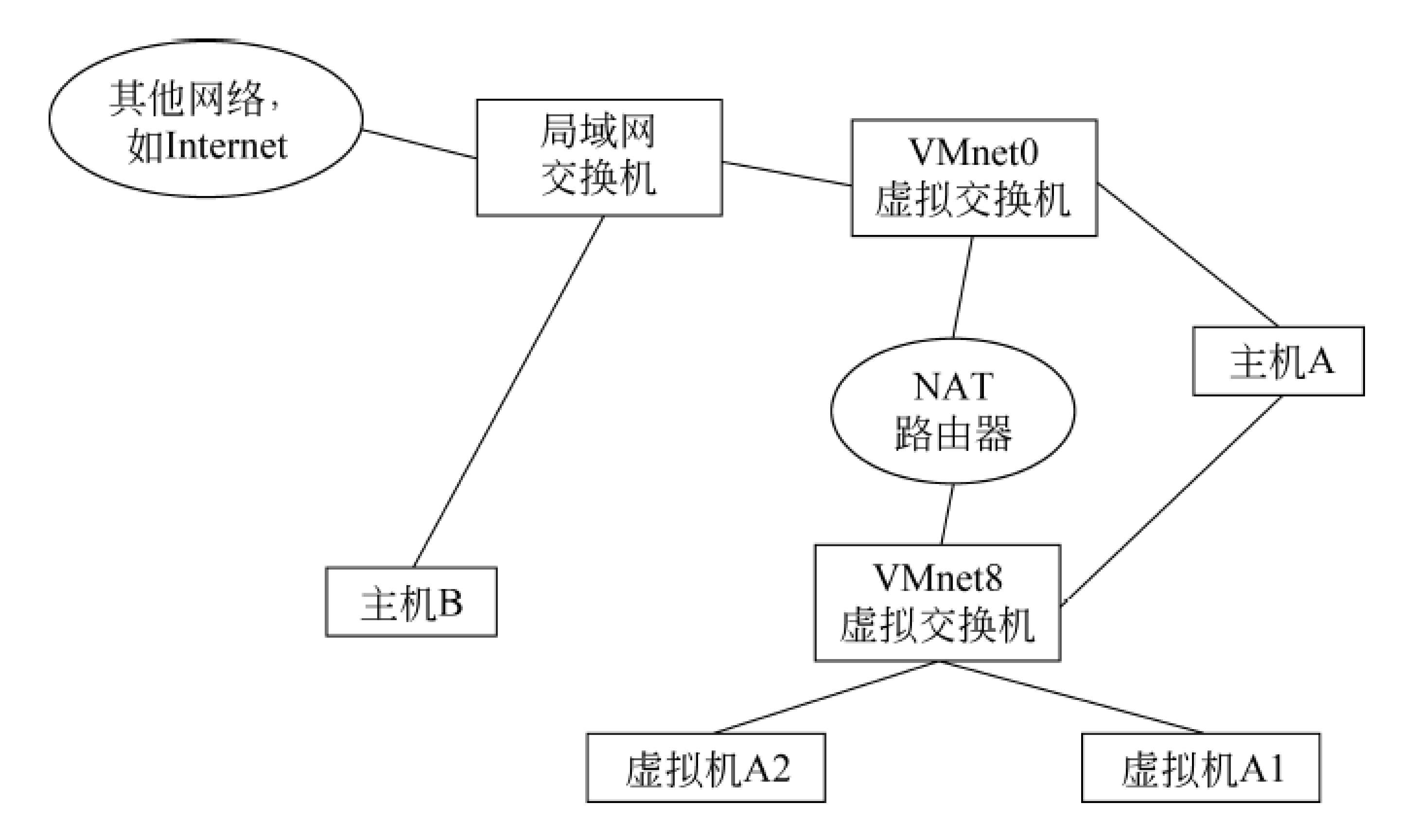


图 13-36 NAT 方式网络拓扑示意图

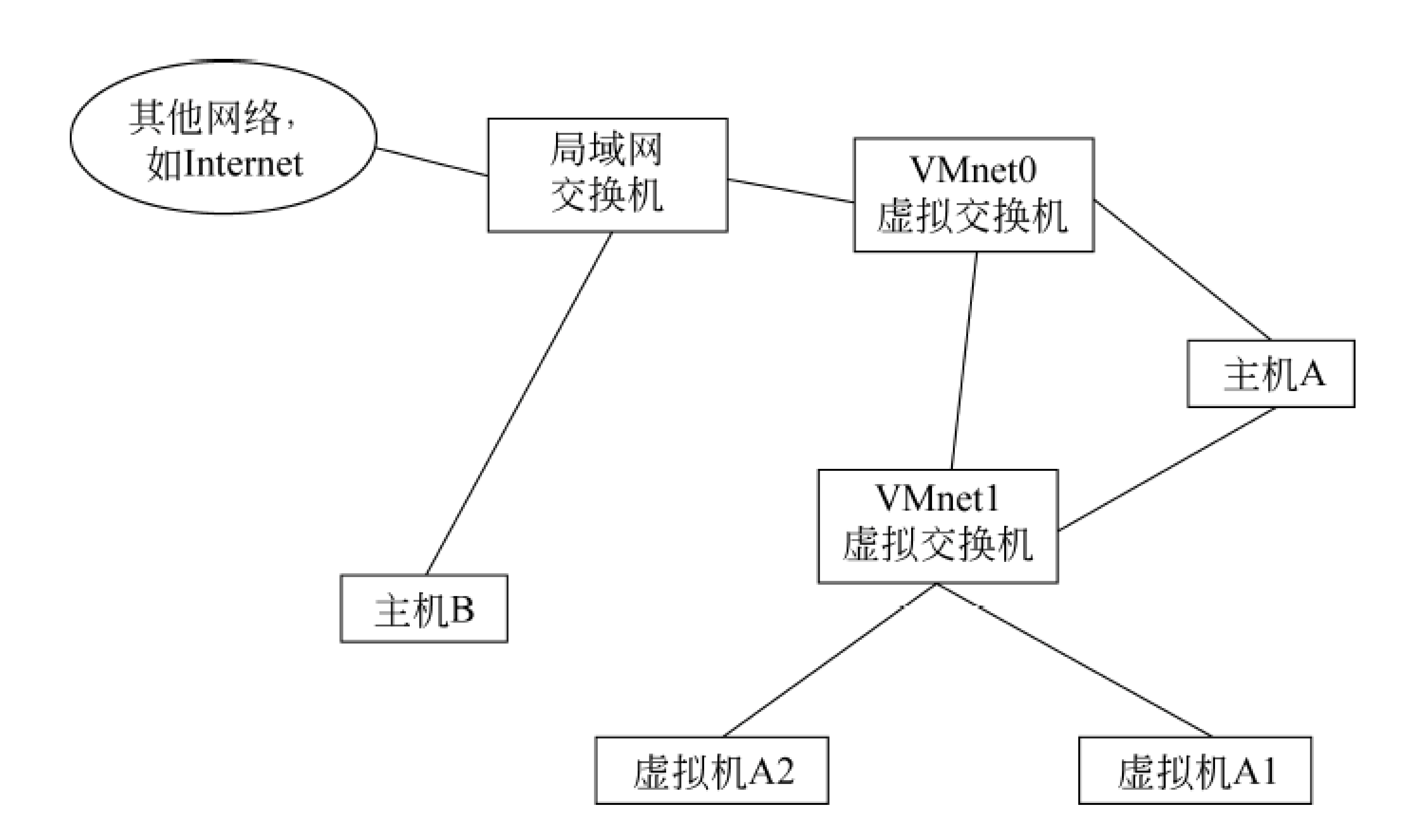


图 13-37 主机网络方式拓扑示意图

参 考 文 献

[1] Microsoft. 网络服务器操作系统的安装、配置和管理[M]. 北京：高等教育出版社，2004.

[2] Microsoft. 网络环境管理[M]. 北京：高等教育出版社，2003.

[3] 戴有炜. Windows Server 2003 用户管理指南[M]. 北京：清华大学出版社，2004.

[4] 戴有炜. Windows Server 2003 活动目录配置指南[M]. 北京：清华大学出版社，2004.

[5] 戴有炜. Windows Server 2003 网络专业指南[M]. 北京：清华大学出版社，2004.

[6] 张素智，崔建涛，等. Windows Server 2003 配置与管理[M]. 郑州：河南科技出版社，2002.